KFU
جامعة الملك فيصل
KING FAISAL UNIVERSITY
جامعة ووطن.. نماء.. واستدامة..

سياسات ومعايير الأمن السيبراني

في جامعة الملك فيصل

معلومات الوثيقة:

اسم الوثيقة	سياسات ومعايير الأمن السيبراني في جامعة الملك فيصل
عدد صفحات الملف	٢٥٠
رقم الإصدار الحالي	٤,١
المراجعة والتحديث	مرة كل (سنتين)أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة من الهيئة الوطنية للأمن السيبراني .
المشاركة	إتاحة المشاركة على مستوى منسوبي جامعة الملك فيصل والجهات ذات العلاقة
تصنيف الوثيقة	مقّيد - للاستخدام الداخلي
ملكية الوثيقة	إدارة الأمن السيبراني
المرجع	الهيئة الوطنية للأمن السيبراني

سجل التغييرات:

رقم الإصدار	التاريخ	ملخص التغيير	مُنفّذ التغيير
٠,٧	٢٠٢٠/١١/١٥ م	إنشاء مسودة الوثيقة	قسم التطوير والجودة بعمادة تقنية المعلومات
١,٠	٢٠٢٠/١٢/١٣ م	الإصدار الأول	
٢,٠	٢٠٢١/٧/١٢ م	الإصدار الثاني - "التحديث على الإصدار الأول"	
٣,٠	٢٠٢١/١٢/٢ م	الإصدار الثالث – "مراجعة وتحديث السياسات"	إدارة الأمن السيبراني
٤,٠	٢٠٢٣/٠١/١٠ م	الإصدار الرابع – "مراجعة وتحديث السياسات"	
٤,١	٢٠٢٣/١١/٨ م	الإصدار الخامس – "مراجعة وتحديث السياسات"	

قائمة الاعتماد:

رقم الإصدار	إعداد	مراجعة	اعتماد	التاريخ
١,٠	قسم التطوير والجودة بعمادة تقنية المعلومات	إدارة الأمن السيبراني	عميد تقنية المعلومات بجامعة الملك فيصل (د. حسن بن شجاع القحطاني)	٢٠٢٠/١٢/٢٤ م
٢,٠				٢٠٢١/٧/١٤ م
٣,٠			تم الاعتماد بمحضر الاجتماع الأول للجنة الدائمة للتحول الرقمي للعام الدراسي ١٤٤٢/١٤٤٣هـ بتاريخ ١٤٤٣/٥/٨ هـ الموافق ٢٠٢١/١٢/١٢ م	٢٠٢١/١٢/١٢ م

٤,٠	إدارة الأمن السيبراني	إدارة الأمن السيبراني	تم الاعتماد بمحضر الاجتماع الثالث للجنة الإشرافية للأمن السيبراني للعام الدراسي ١٤٤٤/١٤٤٣هـ بتاريخ ١٤٤٤/٨/٢٩ هـ الموافق ٢٠٢٣/٣/٢١ م	٢٠٢٣/٣/٢١ م
٤,١	إدارة الأمن السيبراني	إدارة الأمن السيبراني	تم الاعتماد بمحضر الاجتماع الأول للجنة الإشرافية للأمن السيبراني للعام الدراسي ١٤٤٥/١٤٤٤هـ بتاريخ ١٤٤٥/٨/٢٥ هـ الموافق ٢٠٢٤/٣/٧ م	٢٠٢٤/٣/٧ م

قائمة المحتويات

الموضوع **رقم الصفحة**

قائمة الجداول

الجدول | رقم الصفحة

١- مقدمة

إن تعريف الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع. كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحوهما.

وحيث أن الهيئة الوطنية للأمن السيبراني وهي الجهة التنظيمية في الدولة والمعنية بإعداد الاستراتيجية الوطنية للأمن السيبراني والاشراف على تنفيذها، مع وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني وتعميمها على الجهات ذات العلاقة ومتابعة الالتزام بها وتحديثها، بالإضافة إلى إشعار الجهات المعنية بالمخاطر والتهديدات ذات العلاقة بالأمن السيبراني، وذلك بهدف حماية المصالح الحيوية للدولة وأمنها الوطني والبُنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية. حيث طرحت الهيئة الوطنية للأمن السيبراني مجموعة من أدوات الأمن السيبراني لمساعدة الجهات في تطوير ورفع كفاءة الأمن السيبراني وزيادة فعاليته لديها، كما قامت الهيئة بتطوير أدوات الأمن السيبراني (Cybersecurity Toolkit) وهي عبارة عن محتوى يشمل نماذج توضيحية لسياسات ومعايير ووثائق الأمن السيبراني.

هذا وقد تم الأخذ بعين الاعتبار عند إنشاء هذه الوثيقة مجموعة أدوات ونماذج الأمن السيبراني التي طرحتها الهيئة الوطنية للأمن السيبراني، وتهدف هذه الوثيقة إلى تقديم السياسة العامة للأمن السيبراني في جامعة الملك فيصل وذلك بما يتوافق مع الضوابط والأطر التنظيمية ذات العلاقة بالأمن السيبراني في الدولة، وكذلك بما يتناسب مع التقنيات الحديثة المرتبطة بالتحوّل الرقمي وما يتبعها من إجراءات لتأمين وحماية وتعزيز كافة جوانب الأمن السيبراني في أنظمة وخدمات جامعة الملك فيصل.

وقد اشتملت هذه السياسة على مجموعة من السياسات والمعايير الفرعية ذات العلاقة بكافة جوانب الأمن السيبراني، وكذلك الهيكل التنظيمي للأمن السيبراني في الجامعة وما يشمله من أدوار ومسؤوليات الأمن السيبراني، بالإضافة إلى الأعمال والمهام التي تقوم بها اللجنة الإشرافية للأمن السيبراني في الجامعة.

٢- أهداف السياسة العامة

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جامعة الملك فيصل بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأعمال التنظيمية الخاصة بجامعة الملك فيصل، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

٣- نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجامعة الملك فيصل وتنطبق على جميع منسوبي الجامعة.

تعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات جامعة الملك فيصل الداخلية، مثل عمليات الموارد البشرية وعمليات إدارة الموردين وعمليات إدارة المشاريع وإدارة التغيير وغيرها.

٤- عناصر السياسة العامة

١- يجب على إدارة الأمن السيبراني تحديد معايير الأمن السيبراني وتوثيق سياساته وبرامجه، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام جامعة الملك فيصل بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية لجامعة الملك فيصل، والمتطلبات التشريعية والتنظيمية ذات العلاقة. واعتمادها من قبل معالي رئيس الجامعة. كما يجب إطلاع العاملين المعنيين في جامعة الملك فيصل والأطراف ذات العلاقة عليها.

٢- يحق لإدارة الأمن السيبراني الاطلاع على المعلومات، وجمع الأدلة اللازمة للتأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة المتعلقة بالأمن السيبراني.

٣- تشتكل أدوار ومسؤوليات الأمن السيبراني (Responsibilities Cybersecurity Roles and) على وذع وتحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني بما في ذلك الهيكل التنظيمي للأمن السيبراني وأدوار ومسؤوليات أعضاء اللجنة الإشرافية للأمن السيبراني في الجامعة.

٤- يجب على إدارة الأمن السيبراني تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها، والمتمثلة في:

١-٤ **سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (Regulatory Cybersecurity Compliance)** للتأكد من توافق سياسة الأمن السيبراني بالجامعة وما تشمله من تنظيمات مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٤ **سياسة الإعدادات والتحصين** لضمان توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية وتحصين وضبط إعدادات الأصول المعلوماتية والتقنية والتطبيقات الخاصة بالجامعة.

٣-٤ **سياسة الحماية من البرمجيات الضارة** لضمان توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة بالجامعة من تهديدات البرمجيات الضارة وتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية.

٤-٤ **سياسة أمن الخوادم** لضمان توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالخوادم (Servers) الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

٤-٥ **سياسة أمن الشبكات (Networks Security Management)** لضمان حماية شبكات الجامعة من المخاطر السيبرانية.

٤-٦ **سياسة أمن البريد الإلكتروني (Email Protection)** لضمان حماية البريد الإلكتروني الخاص بالجامعة من المخاطر السيبرانية.

٤-٧ **سياسة الاستخدام المقبول للأصول** لضمان توفير متطلبات الأمن السيبراني لتقليل المخاطر السيبرانية المتعلقة باستخدام أنظمة الجامعة وأصولها وحمايتها من التهديدات الداخلية والخارجية والعناية بالأهداف الأساسية للحماية.

٤-٨ **سياسة مراجعة وتدقيق الأمن السيبراني (Assessment and Audit Cybersecurity Periodical)** للتأكد من أن ضوابط الأمن السيبراني لدى الجامعة مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الأخرى المُقرة تنظيمياً بالجامعة.

٤-٩ **سياسة إدارة هويات الدخول والصلاحيات (Management Identity and Access)** لضمان حماية الأمن السيبراني للوصول المنطقي (Access Logical) إلى الأصول المعلوماتية والتقنية للجامعة من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بجامعة الملك فيصل.

٤-١٠ **سياسة الأمن السيبراني للموارد البشرية (Resources Cybersecurity in Human)** للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) في الجامعة تعالج بفعالية قبل إنهاء عملهم، وأثنائه وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٤-١١ **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Logs and Monitoring Cybersecurity Event Management)** لضمان جمع سجلات أحداث الأمن السيبراني، وتحليلها، ومراقبتها في الوقت المناسب من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية لمنع الآثار السلبية المحتملة على أعمال الجامعة أو تقليلها.

٤-١٢ **سياسة إدارة حزم التحديثات والإصلاحات** لضمان تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة بالجامعة.

٤-١٣ **سياسة الأمن السيبراني المتعلق بالأطراف الخارجية (Computing Third-Party and Cloud Cybersecurity)** لضمان حماية أصول الجامعة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٤-١٤ **سياسة اختبار الاختراق (Penetration Testing)** لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في الجامعة، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف

الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني لجامعة الملك فيصل وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٤-١٥ **سياسة إدارة الثغرات (Vulnerabilities Management)** لضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل ذلك، وكذلك تقليل الآثار المترتبة على أعمال الجامعة.

٤-١٦ **سياسة إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)** لضمان اكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب، وإدارتها بشكل فعّال، والتعامل مع تهديدات الأمن السيبراني استباقياً، من أجل منع الآثار السلبية المحتملة أو تقليلها على أعمال الجامعة، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم ٣٧١٤٠ والتاريخ ١٤٣٨/٨/١٤هـ.

٤-١٧ **سياسة أمن قواعد البيانات** لضمان توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية قواعد البيانات (Database) الخاصة بالجامعة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

٤-١٨ **سياسة حماية تطبيقات الويب (Web Application Security)** لضمان حماية تطبيقات الويب الداخلية والخارجية للجامعة من المخاطر السيبرانية.

٤-١٩ **سياسة الأمن السيبراني لأنظمة التحكم الصناعي (Cybersecurity Industrial Control Systems)** لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول الجامعة وسلامتها وسريتها وهي الأصول المتعلقة وأنظمة التحكم الصناعي وأنظمته (OT\ICS) ضد الهجوم السيبراني (مثل الوصول غير المصرح به، والتخريب والتجسس والتلاعب) بما يتسق مع استراتيجية الأمن السيبراني للجامعة، وكذلك إدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الأخرى المتعلقة بالأمن السيبراني والمقرّة تنظيمياً على الجامعة.

٤-٢٠ **سياسة التشفير (Cryptography)** لضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية الخاصة بالجامعة، وذلك وفقاً للسياسات، والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٤-٢١ **سياسة إدارة مخاطر الأمن السيبراني** لضمان تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لإدارة مخاطر الأمن السيبراني في الجامعة، وذلك وفقاً لاعتبارات سرية الأصول المعلوماتية والتقنية وتوافرها وسلامتها.

٤-٢٢ **سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة (Cybersecurity Cloud Computing and Hosting)** لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعّال، وذلك وفقاً للسياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية

والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية للجامعة على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

٢٣-٤ **سياسة إدارة النسخ الاحتياطية (Backup and Recovery Management)** لضمان حماية بيانات الجامعة ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجامعة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢٤-٤ **سياسة حماية وتصنيف البيانات والمعلومات (Data and Information Protection and Classification)** لضمان حماية السرية، وسلامة بيانات ومعلومات الجامعة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢٥-٤ **سياسة الأمن المادي والبيئي (Physical and Environmental Security)** لضمان حماية الأصول المعلوماتية والتقنية للجامعة من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

٢٦-٤ **سياسة إدارة الأصول (Asset Management)** للتأكد من أن جامعة الملك فيصل لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة بالجامعة، من أجل دعم العمليات التشغيلية للجامعة ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية، وسلامتها، ودقتها، وتوافرها.

٥- الأدوار والمسؤوليات

يهدف هذا القسم إلى تحديد المسؤوليات الخاصة بتطبيق برامج ومتطلبات الأمن السيبراني ودعمه وتعزيزه في جامعة الملك فيصل، ويجب على جميع الأطراف المشاركة في تطبيق برامج ومتطلبات الأمن السيبراني فهم أدوارهم والقيام بمسؤولياتهم المتعلقة بالأمن السيبراني في الجامعة، كما يهدف هذا القسم إلى التأكد من أن جميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجامعة على دراية بمسؤولياتهم في تطبيق برامج ومتطلبات الأمن السيبراني في الجامعة، بالإضافة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٤-١ والضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

١- تُمثل القائمة الآتية أبرز مجموعة الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعاييره وبرامجه، وتنفيذها واتباعها، على أن تقوم إدارة الأمن السيبراني متمثلة في المسؤول على إدارة الأمن السيبراني بالتنسيق لعمل التالي:

١-١-١ الرفع لصاحب الصلاحية معالي رئيس الجامعة من أجل تشكيل لجنة إشرافية للأمن السيبراني بالجامعة على أن يكون المسؤول على إدارة الأمن السيبراني أحد أعضاء تلك اللجنة.

١-١-٢ الرفع لصاحب الصلاحية معالي رئيس الجامعة من أجل الحصول على الموافقة على سياسات الأمن السيبراني، والتأكد من إطلاع الأطراف المعنية عليها وتطبيقها، ومراجعتها وتحديثها بشكل دوري.

١-١-٣ الجهة/الجهات المسؤولة عن الموارد البشرية بالجامعة والتي يعمل لديها موظفين متعاقدين من خلال مشاريع تشغيلية، وذلك من أجل تطبيق متطلبات الأمن السيبراني المتعلقة بمنسوبي الجامعة.

١-١-٤ التنسيق مع الجهة المعنية بالشؤون القانونية في الجامعة من أجل التأكد من أن شروط ومتطلبات الأمن السيبراني والمحافظة على سرية المعلومات (Non-disclosure Clauses) مُلزمة قانونياً في عقود منسوبي الجامعة، والأطراف الخارجية.

١-١-٥ التنسيق مع قسم التطوير والجودة والأقسام ذات الصلة في عمادة تقنية المعلومات من أجل مراجعة ضوابط الأمن السيبراني وتدقيق تطبيقها وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١-٦ التنسيق مع كافة جهات الجامعة من أجل دعم سياسات الأمن السيبراني وإجراءاته ومعاييره وبرامجه، وتوفير جميع الموارد المطلوبة لتحقيق الأهداف المنشودة بما يخدم المصلحة العامة لجامعة الملك فيصل، وكذلك العمل على توعية وتعريف منسوبي الجامعة بمتطلبات الأمن السيبراني في الجامعة والالتزام بها.

٦- الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٧- الاستثناءات

يُمنع تجاوز سياسات الأمن السيبراني ومعاييره، دون الحصول على تصريح رسمي مسبق من المسؤول على إدارة الأمن السيبراني أو اللجنة الإشرافية للأمن السيبراني في الجامعة، ما لم يتعارض مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

القسم الأول

أدوار ومسؤوليات وهيكل

الأمن السيبراني

ا- الهيكل التنظيمي للأمن السيبراني

تم إنشاء إدارة الأمن السيبراني وفقاً للمتطلبات التنظيمية الصادرة من الهيئة الوطنية للأمن السيبراني. كما تم تطوير الهيكل التنظيمي للأمن السيبراني بناءً على أفضل الممارسات والمعايير لتوفير الدعم اللازم لإدارة الأمن السيبراني لتمكينها من تنفيذ المهام الموكلة إليها بالشكل المطلوب. وتُعد إدارة الأمن السيبراني أحد الروافد الأساسية في جامعة الملك فيصل وهي المعنية بحماية الأصول المعلوماتية والتقنية من المخاطر السيبرانية. إن الهدف من هذا القسم هو تحديد وتوثيق الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني في جامعة الملك فيصل.

عناصر الهيكل التنظيمي للأمن السيبراني بجامعة الملك فيصل

يستعرض الجدول التالي: (جدول رقم: 1 - عناصر الهيكل التنظيمي للأمن السيبراني بالجامعة) مسميات الوحدات التنظيمية التي تؤثر في أعمال الأمن السيبراني بالجامعة.

م	العنصر	الوصف
١	صاحب الصلاحية	يُعد صاحب الصلاحية (أو من ينيبه) أعلى سلطة في جامعة الملك فيصل.
٢	اللجنة الإشرافية للأمن السيبراني في الجامعة	اللجنة الإشرافية للأمن السيبراني في الجامعة هي مجلس حوكمة رفيع المستوى، وتتمثّل مسؤوليتها الأساسية في ضمان التزام تطبيق برامج وتشريعات الأمن السيبراني داخل جامعة الملك فيصل ودعمها ومتابعتها.
٣	إدارة الأمن السيبراني	إدارة الأمن السيبراني هي الكيان التنظيمي المعني بحماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات، والأمن الإلكتروني، والأمن الرقمي ونحو ذلك.
٤	تقنية المعلومات	عمادة تقنية المعلومات هي المعنية بتشغيل البنية التحتية لتقنية المعلومات والشبكات، وتطوير البرمجيات والخدمات التقنية، وغير ذلك من أعمال.
٥	الموارد البشرية	الجهة / الجهات المعنية بشؤون العاملين والموارد البشرية داخل جامعة الملك فيصل.
٦	الشؤون القانونية	هي الجهة المعنية بالشؤون القانونية في الجامعة بما فيها صياغة العقود والاتفاقيات وحفظ حقوق جامعة الملك فيصل القانونية.
٧	المشتريات	هي الجهة المعنية بإدارة عملية المشتريات والمناقصات في الجامعة بما فيها التعاقد مع الموردين وعمليات الشراء وكذلك عقود الأطراف الخارجية في جامعة الملك فيصل.
٨	الشؤون المالية	هي الجهة المعنية بإدارة عملية التخطيط المالي والميزانية في الجامعة بما في ذلك إعداد الميزانية العامة لجامعة الملك فيصل.
٩	التدقيق والمراجعة الداخلية	هو القسم المعني بتدقيق ومراجعة تطبيق جامعة الملك فيصل للسياسات والإجراءات وكذلك المتطلبات التنظيمية والتشريعية ذات العلاقة بالأمن السيبراني وهو قسم التطوير والجودة بعمادة تقنية المعلومات.
١٠	إدارة استمرارية الأعمال	هي الأقسام ذات العلاقة في عمادة تقنية المعلومات والمعنية بجميع المسائل المتعلّقة باستمرارية الأعمال في جامعة الملك فيصل.
١١	تقنية التشغيل	هي الأقسام ذات العلاقة في عمادة تقنية المعلومات (Operational Technology) وهي المعنية بجميع المسائل المتعلّقة بالتقنية التشغيلية في جامعة الملك فيصل.

م	العنصر	الوصف
١٢	مكتب إدارة المشاريع	هو مكتب إدارة المشاريع بعمادة تقنية المعلومات وهو المعني بجميع المسائل المتعلّقة بإدارة المشاريع التقنية والأمنية في جامعة الملك فيصل.
١٣	وحدات الأعمال	هو مصطلح يشمل جميع قطاعات ووحدات الأعمال والإدارات الأخرى في جامعة الملك فيصل كالعمادات المساندة، والمراكز والكليات، والإدارات.

هيكلية الأمن السيبراني

لتقوم إدارة الأمن السيبراني بعملها بالشكل المطلوب وبكفاءة عالية، تم توزيع المهام والأدوار في إدارة الأمن السيبراني بناءً على الوظائف التشغيلية لكل دور، مع الأخذ بعين الاعتبار مبدأ فصل المهام (Segregation of Duties) وتعارض المصالح (Conflict of Interest) وتم توزيعها كالتالي:

الهيكل التنظيمي إدارة الأمن السيبراني

١- يتولّى الهيكل التنظيمي للأمن السيبراني الإشراف على الميزانية، ويتحمّل مسؤولية التقنية الأمنية والموارد البشرية المعنية بتشغيل وإدارة هذه التقنية.

٢- يتجنّب الهيكل التنظيمي للأمن السيبراني نقل التحكم بالتقنيات الأمنية والذي قد يُعرّض جامعة الملك فيصل إلى مخاطر غير مقبولة.

٣- يُتيح الهيكل التنظيمي للأمن السيبراني استخدام تقنيات متطوّرة تُشجّع الابتكار السريع واعتماد الضوابط الأمنية الجديدة.

٤- يوفر الهيكل التنظيمي للأمن السيبراني مركز عمليات تشغيلي للأمن السيبراني، ويحظى فيه مدير مركز عمليات الأمن السيبراني على عدد أكبر من الموظفين والصلاحيات والسلطات. وذلك وفقاً للجداول التالية:

الحوكمة

يظهر من خلال الجدول التالي: (جدول رقم: ٢ – الأدوار والمسؤوليات المتعلقة بحوكمة الأمن السيبراني) أدوار ومسؤوليات أعمال حوكمة الأمن السيبراني.

م	الأدوار	المسؤوليات
١	إدارة ومراقبة سياسة الأمن السيبراني Cybersecurity Policy Control and Management	التأكّد من توثيق متطلّبات الأمن السيبراني والتزام جامعة الملك فيصل بها وفقاً للمتطلّبات التشريعية والتنظيمية ذات العلاقة.
٢	نشر سياسة الأمن السيبراني والتوعية بها Cybersecurity Policy Communication and Awareness	التأكّد من نشر متطلّبات الأمن السيبراني وفقاً للمتطلّبات التشريعية والتنظيمية ذات العلاقة، وضمان أن العاملين في جامعة الملك فيصل لديهم الوعي الأمني اللازم وأنهم على دراية بمسؤولياتهم في مجال الأمن السيبراني.

م	الأدوار	المسؤوليات
٣	الخصوصية وحماية البيانات Data Protection & Privacy	ضمان حماية سريّة بيانات ومعلومات جامعة الملك فيصل وسلامتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية المعتمدة فيها، ووفقاً للمتطلّبات التشريعية والتنظيمية ذات العلاقة. وكذلك تطوير برنامج الالتزام بالخصوصية وموظفي برنامج الخصوصية والإشراف عليهما، ودعم الالتزام بالخصوصية والحوكمة والسياسة واحتياجات الاستجابة للأحداث للمديرين التنفيذيين وفرقهم المتخصّصة بالخصوصية والأمن.
٤	صمود الأمن السيبراني Cybersecurity Resilience	ضمان توافر متطلّبات صمود الأمن السيبراني في إدارة استمرارية أعمال جامعة الملك فيصل. وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحساسة لجامعة الملك فيصل وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن الأحداث السيبرانية.

المخاطر والالتزام

يتبين من خلال الجدول التالي: (جدول رقم: ٣ - الأدوار والمسؤوليات المتعلقة بالمخاطر والالتزام بالأمن السيبراني) أدوار ومسؤوليات أعمال مخاطر وإدارة الالتزام بالأمن السيبراني.

م	الأدوار	المسؤوليات
١	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	ضمان إدارة مخاطر الأمن السيبراني على نحوٍ منهجي يهدف إلى حماية الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل، وذلك وفقاً للسياسات والإجراءات التنظيمية المعتمدة في جامعة الملك فيصل والمتطلّبات التشريعية والتنظيمية ذات العلاقة.
٢	إدارة الالتزام بالأمن السيبراني Cybersecurity Compliance Management	التأكّد من تنفيذ ضوابط الأمن السيبراني والتزامها بسياسات وإجراءات جامعة الملك فيصل بالإضافة إلى التشريعات، والأنظمة، والاتفاقيات الوطنية، والدولية.

معمارية الأمن السيبراني

يستعرض الجدول التالي: (جدول رقم: ٤ - الأدوار والمسؤوليات المتعلقة بمعمارية الأمن السيبراني) أدوار ومسؤوليات أعمال معمارية الأمن السيبراني.

م	الأدوار	المسؤوليات
١	الاستشارات التقنية المتعلّقة بالأمن السيبراني Technical Cybersecurity Consultancy	تولي مسؤولية وضع التدابير الأمنية التقنية وفقاً لسياسات ومعايير جامعة الملك فيصل، وضمان مراجعة جميع تصاميم تقنية المعلومات واعتمادها من جانب الأمن السيبراني قبل تنفيذها.
٢	استشارات المشاريع Project Consultancy	إدارة مشاريع الأمن السيبراني وتنسيقها ونشرها ودمجها والمساءلة عن نجاحها بشكل عام، وكذلك تقييم المشاريع لضمان التزامها بالمعايير المنشورة.
٣	الأمن السيبراني للتطبيقات Application Cybersecurity	ضمان إدراج المتطلّبات المتعلّقة بالأمن السيبراني ضمن دورة حياة تطوير الأنظمة والبرمجيات.

عمليات الأمن السيبراني

يظهر من خلال الجدول التالي: (جدول رقم: ٥ - الأدوار والمسؤوليات المتعلقة بعمليات الأمن السيبراني) الأدوار والمسؤوليات المتعلقة الأعمال المختلفة في مجال الأمن السيبراني.

م	الأدوار	المسؤوليات
١	الاستجابة لحوادث الأمن السيبراني وتحليلها Cybersecurity Incident Response and Forensics	التعامل مع الكوارث أو الحالات الطارئة ضمن المجال ذي الصلة للتخفيف من التهديدات المباشرة والمحتملة، واستخدام مقاربات التخفيف والاستعداد والاستجابة والتعافي عند اللزوم للحفاظ على الممتلكات والأمن السيبراني بأقصى حدٍّ ممكن، وكذلك التحقيق في جميع أنشطة الاستجابة ذات الصلة وتحليلها. بالإضافة إلى جمع الأدلة المتعلّقة بالحاسوب ومعالجتها وحفظها وتحليلها وتقديمها بما يدعم وسائل التخفيف من ثغرات الشبكة و/أو التحقيقات الجنائية، أو الاحتيالية، أو مكافحة التجسّس، أو إنفاذ القانون.
٢	مراقبة وتحليل الأمن السيبراني Cybersecurity Monitoring and Analysis	ضمان جمع وتحليل ومراقبة أحداث الأمن السيبراني لاكتشاف الهجمات السيبرانية في وقت مبكر بهدف منع أو تقليل الآثار السلبية الناجمة عنها على عمليات جامعة الملك فيصل.
٣	إدارة الثغرات والتهديدات Vulnerability and Threat Management	ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعّال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال جامعة الملك فيصل. وضمان تحديد واكتشاف تهديدات الأمن السيبراني في الوقت المناسب وإدارتها والتعامل معها بفاعلية لمنع أو تقليل الآثار السلبية الناجمة عنها على عمليات جامعة الملك فيصل.
٤	البنية التحتية والعمليات المتعلّقة بالأمن السيبراني Cybersecurity Infrastructure and Operations	تولي مسؤولية تشغيل وإدارة وصيانة حلول الأمن السيبراني وتقنياته وبنيته التحتية وفقاً للمتطلّبات التشريعية والتنظيمية ذات العلاقة.

٢- الأدوار والمسؤوليات المتعلقة بالأمن السيبراني

صاحب الصلاحية (معالي رئيس الجامعة أو من ينيبه)

١. تأسيس إدارة الأمن السيبراني، وتعيين مسؤول على إدارة الأمن السيبراني ويجب أن يكون سعودي الجنسية.
٢. تأسيس اللجنة الإشرافية للأمن السيبراني في الجامعة.
٣. الموافقة على مهام اللجنة الإشرافية للأمن السيبراني في الجامعة.
٤. تخصيص الميزانية الكافية لمتطلبات الأمن السيبراني بما في ذلك ميزانية الموارد البشرية.
٥. اعتماد استراتيجية الأمن السيبراني بعد رفعها للجنة الإشرافية للأمن السيبراني في الجامعة.
٦. اعتماد سياسات الأمن السيبراني بعد رفعها للجنة الإشرافية للأمن السيبراني في الجامعة.
٧. اعتماد حوكمة الأمن السيبراني ومنهجية إدارة المخاطر السيبرانية بعد رفعهما للجنة الإشرافية للأمن السيبراني في الجامعة.
٨. اعتماد منهجية إدارة المخاطر السيبرانية بعد رفعها للجنة الإشرافية للأمن السيبراني في الجامعة.
٩. الاطلاع على تقارير حالة الأمن السيبراني دورياً، وتوفير الدعم المطلوب.

أعضاء اللجنة الإشرافية للأمن السيبراني في الجامعة

١. متابعة المبادئ (Principles) والمتطلبات التشغيلية وفقاً لمهام اللجنة الإشرافية للأمن السيبراني في الجامعة.
٢. ترسيخ مبادئ المساءلة والمسؤولية والصلاحية من خلال تحديد الأدوار والمسؤوليات بهدف حماية الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل.
٣. التأكد من وجود منهجية معتمدة لإدارة وتقييم المخاطر السيبرانية ومستوى المخاطر المقبول (Appetite Risk) لدى جامعة الملك فيصل، ومراجعتها بشكل مستمر أو عند حدوث أي تغيير جوهري في مستوى المخاطر المقبول.
٤. الموافقة على إجراءات مخاطر الأمن السيبراني ودعمها ومراقبتها.
٥. الموافقة على حوكمة الأمن السيبراني ودعمها ومراقبتها.
٦. مراجعة استراتيجية الأمن السيبراني لضمان توافقها مع الأهداف الاستراتيجية لجامعة الملك فيصل قبل اعتمادها.
٧. اعتماد تنفيذ استراتيجية الأمن السيبراني ودعمه ومراقبته.
٨. الموافقة على تطبيق سياسات الأمن السيبراني ودعمه ومراقبته.
٩. اعتماد مبادرات ومشاريع الأمن السيبراني (مثل: برنامج التوعية بالأمن السيبراني، وحماية البيانات والمعلومات، وغيرها) ودعمها ومراقبتها.
١٠. الموافقة على مؤشرات الأداء (Key Performance Indicators "KPIs") ومتابعتها، والتأكد من فعاليتها لأعمال إدارة الأمن السيبراني والعمل على رفع مستوى الأداء.
١١. متابعة تقارير إدارة حزم البيانات والإعدادات ومراقبتها دورياً.
١٢. متابعة إدارة حوادث الأمن السيبراني ودعمها.
١٣. مراجعة التقارير الدورية الصادرة من إدارة الأمن السيبراني والتي تشتمل على مشاريع الأمن السيبراني، والحالة العامة لوضع الأمن السيبراني، والمخاطر السيبرانية الداخلية التي قد تؤثر على عمل جامعة الملك فيصل، وكذلك المخاطر السيبرانية الخارجية والتي قد تؤثر بشكل مباشر أو غير مباشر على أعمال جامعة الملك فيصل، وتقديم الدعم اللازم لمواجهة تلك المخاطر.
١٤. مراجعة التقارير الخاصة بمخاطر الأمن السيبراني ومتابعة معالجتها وتقديم الدعم اللازم لمعالجتها أو العمل على تقليلها.
١٥. مراجعة التقارير الأمنية الخاصة بحوادث الأمن السيبراني وتقديم التوصيات بشأنها.
١٦. مراجعة طلبات الاستثناءات الخاصة بالأمن السيبراني وتقديم التوصيات بشأنها.
١٧. متابعة تقارير حالة حزم التحديثات والإصلاحات الأمنية، وتقييم الثغرات الأمنية على جميع الأصول التقنية والمعلوماتية والتأكد من معالجتها.

١٨. مراجعة نتائج تدقيق الأمن السيبراني الداخلي والخارجي، والتأكد من وجود خطة مناسبة لمعالجة الملاحظات المكتشفة ومتابعتها وتقديم الدعم اللازم لمعالجتها.
١٩. رفع التقارير الدورية عن حالة الأمن السيبراني والدعم المطلوب لصاحب الصلاحية.
٢٠. مراجعة حالة الالتزام بالمتطلبات الداخلية لجامعة الملك فيصل والمتطلبات التشريعية الصادرة من الهيئة الوطنية للأمن السيبراني.

المسؤول على إدارة الأمن السيبراني

١. الإشراف على تطوير استراتيجية الأمن السيبراني وتحديثها.
٢. الإشراف على تطوير وتنفيذ منهجيات وإجراءات مراقبة حوادث الأمن السيبراني، وتوجيه أنشطة الأمن السيبراني ومتابعتها بشكل مستمر ورفع التقارير الخاصة بها.
٣. الإشراف على تطوير وتحديث منهجية وإجراءات إدارة مخاطر الأمن السيبراني.
٤. التأكد من تطوير معايير وإجراءات الأمن السيبراني والموافقة عليها وتطبيقها.
٥. الإشراف على تطوير سياسات الأمن السيبراني وتحديثها بناءً على متطلبات الأمن السيبراني.
٦. التأكّد من توافق إدارة مخاطر الأمن السيبراني مع إدارة المخاطر في جامعة الملك فيصل.
٧. تقديم حلول وتوصيات حول الأمن السيبراني لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية.
٨. تقديم التوجيهات والدعم اللازم ومعالجة المسائل المتعلقة بتخطيط وإدارة الموارد البشرية الخاصة بالأمن السيبراني (مثل: التوظيف والاحتفاظ بالموظفين والتدريب).
٩. الإشراف على تحديد متطلبات الأمن السيبراني وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة والتأكد من الالتزام بها.
١٠. الإشراف على حوادث الاستجابة للأمن السيبراني ورفع التقارير الخاصة بها.
١١. الإشراف على التقييم المستمر للثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات.
١٢. الإشراف على جمع وتحليل المعلومات الاستباقية المتعلقة بالأمن السيبراني من المصادر الوطنية أو المصادر الدولية.
١٣. الإشراف على إجراء اختبارات اختراق دورية على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية لتقييم مستوى الأمن السيبراني.
١٤. الإشراف على إعداد مبادئ تصميم الأمن السيبراني، وتصاميم الأمن السيبراني للأنظمة والشبكات، ومعمارية الأمن السيبراني، مع ضمان المواءمة مع المعمارية المؤسسيةArchitecture (Enterprise).
١٥. الإشراف على إدارة الوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية لجامعة الملك فيصل من خلال تحديد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في جامعة الملك فيصل وتوثيقها وتطبيقها.
١٦. الإشراف على إعداد الميزانية الخاصة بتنفيذ مبادرات ومشاريع الأمن السيبراني.
١٧. التأكد من مراجعة متطلبات الأمن السيبراني دورياً.
١٨. توفير الدعم والإشراف على إعداد آلية مناسبة لقياس مؤشرات الأداء (KPIs) لأعمال الأمن السيبراني ومشاركتها مع اللجنة الإشرافية للأمن السيبراني في الجامعة.
١٩. التواصل مع الهيئة الوطنية للأمن السيبراني و الإدارة العامة للأمن السيبراني بوزارة التعليم وإدارة العلاقة معها.
٢٠. الإشراف على برامج الأمن السيبراني ومنها برنامج التوعية بالأمن السيبراني.

موظفو إدارة الأمن السيبراني

١. تطوير وتحديث سياسات ومعايير الأمن السيبراني
٢. مراقبة أحداث الأمن السيبراني للبنية التقنية.
٣. إعداد وتطبيق برنامج التوعية بالأمن السيبراني.
٤. إجراء تقييم مخاطر الأمن السيبراني.
٥. مسح الثغرات الأمنية للبنية التقنية.

٦. إدارة الصلاحيات وهويات الدخول.
٧. إجراء التحقق من الالتزام بالسياسات وتشريعات الأمن السيبراني .

عميد تقنية المعلومات

١. التأكد من التزام عمادة تقنية المعلومات بجميع متطلبات الأمن السيبراني.
٢. قيادة وتوجيه موظفي عمادة تقنية المعلومات من خلال الإشراف على التدريب والتوعية والتثقيف بالأمن السيبراني تماشياً مع مسؤولياتهم.
٣. المشاركة والمساهمة في تطوير إطار وإجراءات وعمليات إدارة المخاطر وتطبيقها.
٤. اعتماد وسائل يدوية (غير آلية) للتحديثات والإصلاحات في حال لم تكن الأدوات الآلية المستخدمة في جامعة الملك فيصل مدعومة.
٥. الإشراف والمتابعة الدورية لتنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات.
٦. مراجعة فاعلية وكفاءة إدارة التحديثات والإصلاحات في الأنظمة الحساسة المتعلقة بتقنية المعلومات.
٧. التأكد من إشراك إدارة الأمن السيبراني في جميع المسائل المتعلقة بالأصول المعلوماتية والتقنية، وإدارة المشاريع، والمشتريات.
٨. التأكد من إشراك إدارة الأمن السيبراني لضمان حماية الأصول المعلوماتية والتقنية لجامعة الملك فيصل على النحو المطلوب.
٩. التأكّد من مراجعة عقود الصيانة الحالية مع موردي أنظمة تقنية المعلومات و/أو الأنظمة الحسّاسة لتزويد جامعة الملك فيصل بأحدث الإصدارات من حزم التحديثات والإصلاحات.
١٠. الإشراف على سرعة تطبيق التوصيات للتقليل من مخاطر الأمن السيبراني.
١١. الإشراف على إدارة عمليات التشغيل للأصول التقنية المتعلقة بالأمن السيبراني.

موظفو عمادة تقنية المعلومات

١. تطبيق متطلبات الأمن السيبراني المتعلقة بعمادة تقنية المعلومات، بما في ذلك سياسات الأمن السيبراني وإجراءاته، وعملياته، ومعاييره، وإرشاداته.
٢. معالجة الثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات.
٣. تطبيق متطلبات الأمن السيبراني فيما يتعلق بطبيعة عمل الموظف المعني.
٤. تصعيد أي أنشطة مشبوهة أو مخاوف تتعلق بالأمن السيبراني إلى إدارة الأمن السيبراني والإبلاغ عنها.
٥. المساعدة في تقديم مدخلات لأنشطة عمليات إطار إدارة المخاطر والوثائق ذات العلاقة.
٦. التنسيق مع إدارة الأمن السيبراني حول جميع المسائل المتعلقة بالأصول المعلوماتية والتقنية وإدارة المشاريع.
٧. التنسيق مع إدارة الأمن السيبراني لضمان حماية الأصول المعلوماتية والتقنية لجامعة الملك فيصل وتأمينها على النحو المطلوب.
٨. مراجعة عقود الصيانة الحالية مع موردي أنظمة تقنية المعلومات والأنظمة الحسّاسة للتأكد من تزويد جامعة الملك فيصل بأحدث الإصدارات من حزم التحديثات والإصلاحات.

رئيس قسم النظم والتطبيقات بعمادة تقنية المعلومات

١. الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بتطوير التطبيقات في جامعة الملك فيصل.
٢. التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على قسم النظم والتطبيقات بعمادة تقنية المعلومات.
٣. التأكد من تطبيق معايير الأمن السيبراني المعتمدة لتطوير التطبيقات، مثل (Application Security Project "OWASP" Open Web).
٤. الإشراف على تطبيق معايير وأدوات الاختبار الأمني (Testing Standards) والمعايير الأمنية لشفرة البرامج والتطبيقات (Coding Standards)، بما في ذلك الفحص العشوائي (Fuzzing) لأدوات التحليل الثابت للشفرات (Static Code Analysis) وإجراء مراجعات لشفرة البرامج والتطبيقات (Code Reviews).
٥. تحديد حزم التحديثات والإصلاحات وتوثيقها والتأكد من سلامتها قبل تنصيبها.
٦. التأكد من توثيق الشفرة المصدرية لعمليات التطوير الداخلية والخارجية (أي من خلال طرف خارجي) للتطبيقات في جامعة الملك فيصل لتمكين عمليات التتبع والمراجعة في إدارة الثغرات.
٧. التأكد من البرمجة الآمنة من خلال التأكد من معالجة الأخطاء وتحديد الأخطاء المحتملة في التشفير للحد من الثغرات.

٨. التأكد من معالجة جميع الثغرات في مرحلة بيئة الاختبار (Software Acceptance Phase)، بما في ذلك معايير الإتمام (Completion Criteria)، وقبول المخاطر وتوثيقها، والمعايير المشتركة (Common Criteria)، وأساليب الاختبار المستقل (Independent Testing)، وإطلاع إدارة الأمن السيبراني على جميع مشاريع تطوير التطبيقات.

٩. التأكد من تحديد الخدمات والوظائف المتعلقة بالأمن السيبراني (مثل: التشفير، والتحكم بالوصول، وإدارة الهوية) واستخدامها للحد من فرص الاستغلال.

المعنيون بتطوير التطبيقات

بالإضافة إلى جميع المسؤوليات المذكورة لموظفي عمادة تقنية المعلومات، يتولّى المعنيون بتطوير التطبيقات المسؤوليات التالية:

١. تنفيذ متطلبات الأمن السيبراني المتعلقة بتطوير التطبيقات في جامعة الملك فيصل، واتباع المعايير والإجراءات المعتمدة في تطوير التطبيقات (مثل: معايير التطوير الآمن للتطبيقات).

٢. متابعة عمليات إدارة المشاريع والتغييرات في جامعة الملك فيصل، وذلك بالنسبة لجميع التغييرات التي تنطبق على التطبيقات الخاصة بجامعة الملك فيصل.

٣. تحديد التحديثات والإصلاحات اللازمة للبرامج وتوثيقها.

٤. إجراء البرمجة الآمنة، ومعالجة الأخطاء، وتحديد الأخطاء المحتملة في التشفير للحد من الثغرات.

٥. تطبيق معايير وأدوات الاختبار الأمني والمعايير الأمنية لشفرة البرامج والتطبيقات، بما في ذلك الفحص العشوائي لأدوات التحليل الثابت للشفرات، وإجراء مراجعات لشفرة البرامج والتطبيقات.

٦. تحديد وتوثيق التحديثات والإصلاحات اللازمة للبرامج، والإصدارات التي تكون خلالها البرامج عرضة للثغرات.

رئيس قسم الشبكات ونظم التشغيل بعمادة تقنية المعلومات

١. تنسيق فترات الصيانة حسب الأولوية وتخطيطها وتحديد موعدها من أجل تثبيت التحديثات والإصلاحات وفقاً لسياسة إدارة المشاريع والتغييرات المعتمدة في جامعة الملك فيصل بما لا يؤثر على الأمن السيبراني للأصول.

٢. الإشراف على الحلول الآلية لإدارة حزم التحديثات والإصلاحات، والتأكد من إجراء التحديثات اليدوية في حال كانت التحديثات والإصلاحات الآلية غير مدعومة.

٣. الإشراف على النسخ الاحتياطية المنتظمة واختبارات النسخ الاحتياطية.

٤. الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بعمليات تقنية المعلومات في جامعة الملك فيصل.

٥. التأكد من اختبار تحديثات وإصلاحات الأصول المعلوماتية والتقنية قبل النشر.

٦. التأكد من نجاح تثبيت التحديثات والإصلاحات على الأنظمة.

٧. التأكد من تنفيذ سياسات الأمن السيبراني المتعلقة بالأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل (مثل نموذج سياسة أمن أجهزة المستخدمين، ونموذج سياسة أمن الخوادم، وغيره).

٨. تحديد وترتيب الأولويات والقدرات لاستعادة الأنظمة ووحدات الأعمال الأساسية اللازمة كلياً أو جزئياً بعد وقوع حدث كارثي يؤثر على الأنظمة واستمرارية الأعمال.

٩. تحديد المستويات الملائمة لتوافر المعلومات في الأنظمة، وذلك استناداً إلى الوظائف الأساسية للنظام المعني، مع ضمان أن متطلبات النظام تحدد متطلبات التعافي من الكوارث واستمرارية الأعمال، بما في ذلك أي متطلبات موقع بديل (Fail-over Site)، ومتطلبات النسخ الاحتياطية، ومتطلبات القدرة على الدعم لاستعادة واسترداد النظام.

١٠. الإشراف على اختبار كفاءة خطة التعافي من الكوارث والمشاركة في اختبار كفاءة خطة استمرارية الأعمال.

موظفو قسم الشبكات ونظم التشغيل بعمادة تقنية المعلومات

بالإضافة إلى جميع المسؤوليات المذكورة لموظفي عمادة تقنية المعلومات، يتولّى المعنيون بعمليات تقنية المعلومات المسؤوليات التالية:

١. المساعدة في التنسيق مع إدارة الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بعمليات تقنية المعلومات.

٢. تنفيذ متطلبات الأمن السيبراني المتعلقة بعمليات تقنية المعلومات في جامعة الملك فيصل.

٣. تنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات.

٤. توفير النسخ الاحتياطية واختبارها دورياً.

٥. تنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات، والتأكد من إجراء التحديثات اليدوية متى ما كانت التحديثات والإصلاحات الآلية غير مدعومة.

٦. تفعيل وحماية السجلات المناسبة ودمجها مع نظام إدارة السجلات المركزي.

٧. تهيئة جميع برامج الإدارة وبرامج الحماية ونظام التشغيل على الأصول المعلوماتية والتقنية.

٨. الإشراف على صلاحيات الوصول وحسابات المستخدمين للأصول المعلوماتية والتقنية حسب السياسة الخاصة بها.

٩. مراعاة عزل الأصول المعلوماتية والتقنية والتقسيم المنطقي لأجزاء الشبكات بشكل آمن.

١٠. المشاركة في إدارة التهديدات والحوادث في أنظمة تقنية المعلومات في المراحل المعنية بها (مثل: مراحل الاحتواء (Containment)، والاستئصال (Eradication)، والتعافي أو الاستعادة (Recovery)).

١١. المساعدة في تحديد وترتيب أولويات قدرات الأنظمة ووحدات الأعمال الأساسية اللازمة لاستعادة النظام المعني كلياً أو جزئياً بعد وقوع حدث كارثي يتسبب في فشل متعلق بالأمن السيبراني.

١٢. المساعدة في تحديد المستويات الملائمة لتوافر المعلومات في الأنظمة، وذلك استناداً إلى الوظائف الأساسية للنظام المعني، مع ضمان أن متطلبات النظام تحدد متطلبات التعافي من الكوارث واستمرارية الأعمال، بما في ذلك أي متطلبات موقع بديل (Fail-over Site)، ومتطلبات النسخ الاحتياطية، ومتطلبات القدرة على الدعم لاستعادة النظام واسترداده.

صاحب الصلاحية في الجهة / الجهات المسؤولة عن الموارد البشرية

١. الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في جامعة الملك فيصل.
٢. التأكد من إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة بالتنسيق مع الجهات المعنية.
٣. تولي المسؤولية المتعلقة بدعم تطبيق سياسة الاستخدام المقبول للأصول وتطبيق العقوبات على المخالفين حسب الإجراءات المعتمدة لدى جامعة الملك فيصل.
٤. تولي المسؤولية المتعلقة بسياسة الأمن السيبراني للموارد البشرية مما يترتب على تحديث السياسة ومراجعتها.
٥. حضور اجتماعات اللجنة الإشرافية للأمن السيبراني في الجامعة والمشاركة بها حسب الضرورة.
٦. المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بالأمن السيبراني، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.
٧. إجراء تقييمات الاحتياجات التعليمية وتحديد المتطلبات المتعلقة بالأمن السيبراني.
٨. التأكد من إعداد وتنفيذ أدوار ومسؤوليات وظيفية قياسية وفقاً للأدوار الوظيفية المحددة المتعلقة بالأمن السيبراني.
٩. تحديد المسارات المهنية للأمن السيبراني لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني.
١٠. التنسيق مع إدارة الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على عمادة شؤون أعضاء هيئة التدريس.
١١. المشاركة في مراجعة استراتيجية وسياسات الأمن السيبراني وتقديم المدخلات لها.
١٢. التعامل مع مخالفات عدم الالتزام بسياسات الأمن السيبراني وذلك بالتنسيق مع الإدارة العامة للشؤون القانونية.

موظفو الجهة / الجهات المسؤولة عن الموارد البشرية

١. تنفيذ متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في جامعة الملك فيصل.
٢. إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة بالتنسيق مع الجهات المعنية.
٣. إجراء تقييم للوعي الأمني لجميع العاملين وتحديد نقاط الضعف المتعلقة بالأمن السيبراني والعمل على معالجتها.
٤. تنفيذ برنامج التوعية والتدريب بالأمن السيبراني بالتنسيق مع الإدارة المعنية بالتوعية والتدريب بالأمن السيبراني.
٥. إعداد وتنفيذ أوصاف وظيفية قياسية وفقاً للأدوار الوظيفية المحددة المتعلقة بالأمن السيبراني.
٦. المساعدة في تحديد المسارات المهنية للأمن السيبراني لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني.
٧. تقديم الدعم في المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بالأمن السيبراني، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.

رئيس قسم التطوير والجودة بعمادة تقنية المعلومات

١. الإشراف على المراجعة والتدقيق الدوري لبرامج ومتطلبات الأمن السيبراني وفقاً لمعايير التدقيق المتعارف عليها والمقبولة عموماً، والقوانين والتنظيمات ذات العلاقة.
٢. الإشراف على تدقيق الأمن السيبراني وفقاً لشروط سياسة تدقيق ومراجعة الأمن السيبراني.
٣. التأكد من المراجعة والتحديث الدوري لجميع الوثائق المتعلقة بالأمن السيبراني.
٤. حضور اجتماعات اللجنة الإشرافية للأمن السيبراني في الجامعة والمشاركة بها حسب الضرورة.
٥. التأكد من تحديث مخاطر الأمن السيبراني وإعادة تقييمها وفقاً لسياسة إدارة مخاطر الأمن السيبراني.
٦. التأكد من مواءمة قبول المخاطر مع سياسة إدارة مخاطر الأمن السيبراني.
٧. اقتراح خطّة معالجة لنتائج وملاحظات التدقيق.
٨. توثيق النتائج والملاحظات والإبلاغ عنها ومناقشتها مع الإدارة المعنية.
٩. تقديم نتائج وملاحظات التدقيق إلى المسؤول على إدارة الأمن السيبراني .

١٠. مناقشة الإجراءات التصحيحية مع مسؤولي نتائج التدقيق وتوثيقها.
١١. الإبلاغ عن أي ضوابط غير فعّالة متعلّقة بالأمن السيبراني.
١٢. الإبلاغ عن عدم الالتزام بمتطلبات الأمن السيبراني.
١٣. التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالتدقيق الداخلي.
١٤. مراجعة استراتيجية وسياسات الأمن السيبراني وتقديم المدخلات لها.

موظفو قسم التطوير والجودة بعمادة تقنية المعلومات

١. المساعدة في مراجعة وتدقيق تنفيذ ضوابط الأمن السيبراني وفقاً لمعايير التدقيق المتعارف عليها والمقبولة عموماً، والقوانين والتنظيمات ذات العلاقة.
٢. تنفيذ متطلبات الأمن السيبراني المتعلقة بالتدقيق الداخلي في جامعة الملك فيصل.
٣. المراجعة والتحديث الدوري لجميع الوثائق المتعلقة بالأمن السيبراني.
٤. إجراء مراجعات للتأكّد من تحديث مخاطر الأمن السيبراني وإعادة تقييمها وفقاً لسياسة إدارة مخاطر الأمن السيبراني.
٥. إجراء مراجعات للتأكد من مواءمة قبول المخاطر مع سياسة إدارة مخاطر الأمن السيبراني.
٦. إجراء مراجعات وإبلاغ رئيس التدقيق الداخلي بعدم الالتزام بمتطلبات الأمن السيبراني.
٧. تنفيذ عملية تدقيق الأمن السيبراني وفقاً لشروط سياسة تدقيق ومراجعة الأمن السيبراني.
٨. تحليل الضوابط الفعالة للأمن السيبراني، وتقديم التوصيات لرئيس التدقيق الداخلي بشأنها.
٩. اقتراح الإجراءات التصحيحية على رئيس التدقيق الداخلي وفقاً لنتائج وملاحظات التدقيق.
١٠. المساعدة في اقتراح خطّة معالجة لنتائج وملاحظات التدقيق.
١١. المساعدة في التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالتدقيق الداخلي.

صاحب الصلاحية في الجهة المسؤولة عن الشؤون القانونية في الجامعة

١. حصر المتطلبات التنظيمية والتشريعية الوطنية ذات العلاقة بالأمن السيبراني، والاتفاقيات والالتزامات الدولية المعتمدة محلياً التي تتضمن متطلبات خاصة بالأمن السيبراني تنطبق على جامعة الملك فيصل.
٢. ترجمة ضوابط الأمن السيبراني وتنظيماته وسياساته ومعاييره وإجراءاته، وجعلها ملزمة قانونياً.
٣. التأكد من أن الشروط والأحكام وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) ملزمة للموظفين وللأطراف الخارجية من أجل حماية الأصول المعلوماتية والتقنية لجامعة الملك فيصل.
٤. الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بالشؤون القانونية في جامعة الملك فيصل.
٥. حضور اجتماعات اللجنة الإشرافية للأمن السيبراني في الجامعة والمشاركة بها حسب الضرورة.
٦. تقييم فعالية قوانين وتنظيمات الأمن السيبراني.
٧. مراجعة سياسة أمن الأطراف الخارجية المعتمدة في جامعة الملك فيصل وفقاً للمتطلّبات القانونية ذات العلاقة.
٨. العمل مع إدارة الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالشؤون القانونية.
٩. تقديم الدعم لحوادث الأمن السيبراني عند الحاجة.

موظفو الجهة المسؤولة عن الشؤون القانونية في الجامعة

١. المساعدة في تفسير قوانين الأمن السيبراني وتنظيماته وسياساته ومعاييره وإجراءاته وتطبيقها على مسائل محددة.
٢. تنفيذ متطلبات الأمن السيبراني المتعلقة بالشؤون القانونية في جامعة الملك فيصل.
٣. المساعدة في تقييم فعالية قوانين وتنظيمات الأمن السيبراني.

جميع منسوبي الجامعة

١. التعامل مع البيانات والمعلومات حسب مستوى تصنيفها.
٢. تلافي انتهاك حقوق أي شخص أو شركة محمية بحقوق النشر أو براءة الاختراع أو أي ملكية فكرية أخرى أو قوانين أو لوائح مماثلة.
٣. الالتزام بسياسات وإجراءات الأمن السيبراني.
٤. الالتزام بمتطلبات الأمن السيبراني المتعلقة بحماية أجهزة المستخدمين.
٥. الالتزام بمتطلبات الأمن السيبراني المتعلقة باستخدام الإنترنت والبرمجيات.
٦. الالتزام بمتطلبات الأمن السيبراني المتعلقة بالبريد الإلكتروني.
٧. الالتزام بالمتطلبات المتعلقة بنظم وتقنيات حماية الأمن السيبراني.
٨. استخدام جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل لأغراض العمل فقط وحسب سياسة الاستخدام المقبول للأصول المعتمدة في جامعة الملك فيصل.
٩. الحصول على التصريح المطلوب من إدارة الأمن السيبراني أو صاحب الصلاحية في جامعة الملك فيصل قبل استضافة الزوار في المواقع الحساسة المحددة في جامعة الملك فيصل.
١٠. الإبلاغ عن حوادث الأمن السيبراني.
١١. الالتزام بسياسة الاستخدام المقبول.

٣- اللجنة الإشرافية للأمن السيبراني في الجامعة

تُعد اللجنة الإشرافية للأمن السيبراني في الجامعة كلجنة مختصة لضمان مواءمة استراتيجية إدارة الأمن السيبراني مع الأهداف الاستراتيجية لجامعة الملك فيصل، بالإضافة إلى أهدافها الموكلة إليها في هذه الوثيقة، وتتكون من أصحاب المصلحة المعنيين المسؤولين عن مختلف قطاعات الأعمال في جامعة الملك فيصل، والذين يتحملون مسؤولية التوجيه والدعم وتحديد أولويات والأهداف الاستراتيجية للأمن السيبراني وترتيبها.

التكليف

يتم تأسيس اللجنة الإشرافية للأمن السيبراني في الجامعة بتوجيه من معالي رئيس الجامعة، ويتم تحديد مهامها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة (مثل: الضوابط الأساسية للأمن السيبراني "ECC-1:2018"). وهي متطلب تشريعي في الضابط رقم ١-٢-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

تُقدّم اللجنة الإشرافية للأمن السيبراني في الجامعة إطاراً لحوكمة الأمن السيبراني، ومن الممكن أن يقوم معالي رئيس الجامعة بتكليف اللجنة بمسؤوليات إضافية.

الأهداف

الغرض من وجود اللجنة الإشرافية للأمن السيبراني في الجامعة هو ضمان الالتزام بتطبيق برامج وتشريعات واستراتيجية الأمن السيبراني الخاصة بجامعة الملك فيصل ودعمها ومتابعتها.

الأدوار والمسؤوليات

تعمل اللجنة الإشرافية للأمن السيبراني في الجامعة باعتبارها لجنة مختصة في مناقشة توجّهات الأمن السيبراني وقراراته وأدائه على مستوى الجامعة. كما تتابع اللجنة تنفيذ برامج الأمن السيبراني، وتضمن الالتزام الداخلي باستراتيجية الأمن السيبراني وسياساته وتشريعاته، وتقدّم الدعم المناسب عند الحاجة. وتتضمن مسؤوليات اللجنة على سبيل المثال المهام التالية:

١- متابعة المبادئ والمتطلبات التشغيلية وفقاً لمهام اللجنة.

٢- ترسيخ مبادئ المساءلة والمسؤولية والسلطة من خلال تحديد الأدوار والمسؤوليات بهدف حماية الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل.

٣- التأكد من وجود منهجية معتمدة لإدارة وتقييم المخاطر السيبرانية ومستوى المخاطر المقبول (Risk Appetite) لدى جامعة الملك فيصل.

٤- الموافقة على إجراءات مخاطر الأمن السيبراني ودعمها ومراقبتها.

٥- الموافقة على حوكمة الأمن السيبراني ودعمها ومراقبتها.

٦- مراجعة واعتماد استراتيجية الأمن السيبراني بهدف ضمان توافقها مع الأهداف الاستراتيجية للجامعة.

٧- اعتماد تنفيذ استراتيجية الأمن السيبراني ودعمها ومراقبتها.

٨- الموافقة على تطبيق سياسات الأمن السيبراني ودعمها ومراقبتها.

٩- اعتماد مبادرات ومشاريع الأمن السيبراني (مثل: برنامج التوعية بالأمن السيبراني، وحماية البيانات والمعلومات، وغيرها) ودعمها ومراقبتها.

١٠- الموافقة على مؤشرات الأداء (Key Performance Indicators "KPIs") ومتابعتها، ومتابعة فعاليتها لأعمال إدارة الأمن السيبراني، والعمل على رفع مستوى الأداء.

١١- متابعة تقارير إدارة حزم البيانات والإعدادات ومراقبتها دورياً.

١٢- متابعة إدارة حوادث الأمن السيبراني ودعمها.

١٣- مراجعة التقارير الدورية الصادرة من إدارة الأمن السيبراني والتي تشتمل على مشاريع الأمن السيبراني، والحالة العامة لوضع الأمن السيبراني، والمخاطر المتبقية إثر قبول المخاطر السيبرانية، وكذلك المخاطر السيبرانية التي قد تؤثر بشكل مباشر أو غير مباشر على أعمال الجامعة، مع تقديم الدعم اللازم لمواجهة تلك المخاطر.

١٤- مراجعة التقارير الخاصة بمخاطر الأمن السيبراني ومتابعة معالجتها وتقديم الدعم اللازم لمعالجتها أو التقليل منها.

١٥- مراجعة التقارير الأمنية الخاصة بحوادث الأمن السيبراني وتقديم التوصيات بشأنها.

١٦- مراجعة طلبات الاستثناءات الخاصة بالأمن السيبراني وتقديم التوصيات بشأنها.

١٧- متابعة تقارير حالة حزم التحديثات والإصلاحات الأمنية وتقييم الثغرات الأمنية في جميع الأصول التقنية والمعلوماتية والتأكد من معالجتها.

١٨- مراجعة نتائج تدقيق الأمن السيبراني الداخلي والخارجي، والتأكد من وجود خطة مناسبة لمعالجة الملاحظات المكتشفة ومتابعتها وتقديم الدعم اللازم لمعالجتها.

١٩- رفع التقارير الدورية عن حالة الأمن السيبراني والدعم المطلوب لصاحب الصلاحية.

٢٠- مراجعة حالة الالتزام بالمتطلبات الداخلية لجهات الجامعة والمتطلبات التشريعية الصادرة من الهيئة الوطنية للأمن السيبراني.

تشكيل اللجنة

١- يتولّى رئاسة اللجنة الإشرافية للأمن السيبراني في الجامعة معالي رئيس الجامعة أو من يفوضه.

٢- تتكوّن اللجنة الإشرافية للأمن السيبراني في الجامعة من أعضاء دائمين بالإضافة إلى أعضاء غير دائمين (تتم دعوتهم لحضور اجتماعات اللجنة حسب الحاجة). ويجب أن تشمل اللجنة على أعضاء مسؤولين مؤثرين أو تتأثر أعمالهم بالأمن السيبراني لدى الجامعة، كما في الجدول أدناه (جدول رقم: ٦ – جدول تشكيل عضوية اللجنة الإشرافية للأمن السيبراني في الجامعة).

الوصف الوظيفي	المنصب
معالي رئيس الجامعة	رئيساً للجنة
سعادة وكيل الجامعة للدراسات والتطوير وخدمة المجتمع	عضواً ونائباً للرئيس
سعادة وكيل الجامعة للشؤون الأكاديمية	عضواً
سعادة وكيل الجامعة للدراسات العليا والبحث العلمي	عضواً
سعادة وكيل الجامعة	عضواً
سعادة عميد شؤون أعضاء هيئة التدريس	عضواً
سعادة عميد التعلم الإلكتروني والتعليم عن بعد	عضواً
سعادة عميد تقنية المعلومات	عضواً
سعادة المشرف على إدارة المراجعة الداخلية	عضواً
سعادة المسؤول على إدارة الأمن السيبراني	عضواً ومقرراً

قواعد عامة

١- يجب أن تُعقَد اجتماعات اللجنة ٤ مرات سنوياً على الأقل (مرة كل ثلاثة أشهر)، ويُمكن عقد اجتماعات طارئة إضافية عند الضرورة.

٢- لا يمكن عقد اجتماعات اللجنة الإشرافية للأمن السيبراني في الجامعة دون حضور رئيس اللجنة (أو من ينيبه)، أو في حال عدم حضور أكثر من نصف الأعضاء الدائمين.

٣- في حال تطلب النقاش استضافة خبير أو مستشار في مجال معين، يحق لأمين اللجنة تنسيق الاستضافة بعد الحصول على موافقة رئيس اللجنة.

٤- يحق لأمين اللجنة طلب اجتماعات طارئة خارج الجدولة الرسمية بعد الحصول على موافقة رئيس اللجنة.

٥- يتولى تسجيل محاضر الاجتماعات موظف يتم اختياره بواسطة رئيس اللجنة، على أن تكون جميع محاضر اللجنة موثقة بشكل رسمي ومعتمدة.

٦- تتم مشاركة المعلومات بين أعضاء اللجنة الإشرافية للأمن السيبراني في الجامعة باستخدام بروتوكول الإشارة الضوئية (TLP) من أجل تمكين الحوكمة الآمنة للمعلومات، ويجب تصنيف جميع المعلومات ومحاضر الاجتماعات التي تتم مشاركتها في اللجنة وترميزها بشكل واضح وفقاً للألوان التالية:

٦-١ لا يمكن لأعضاء اللجنة مناقشة المعلومات المصنّفة باللون الأحمر مع أي فرد من خارج اللجنة.

٦-٢ يُمكن لأعضاء اللجنة مشاركة المعلومات المصنّفة باللون البرتقالي مع مرؤوسيهم المباشرين على أساس الحاجة إلى المعرفة للتعامل مع موضوع أو خطر معيّن.

٦-٣ المعلومات المصنّفة باللون الأخضر هي معلومات داخلية يُمكن مشاركتها مع جميع منسوبي الجامعة.

القسم الثاني

مجموعة سياسات

الأمن السيبراني

١. سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من توافق سياسة الأمن السيبراني بالجامعة وما تشمله من تنظيمات مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٧-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة والإجراءات الخاصة بجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- يجب تحديد قائمة التشريعات والتنظيمات المتعلقة بالأمن السيبراني والمتطلبات ذات الصلة وتوثيقها وتحديثها دورياً.

٢- يجب توفير التقنيات اللازمة للتحقق من الالتزام بمتطلبات الجهات التشريعية والتنظيمية المتعلقة بالأمن السيبراني.

٣- يجب مراجعة سياسات الأمن السيبراني وإجراءاته دورياً لضمان التزامها بالمتطلبات التشريعية والتنظيمية ذات العلاقة.

٤- يجب التأكد من تطبيق سياسات الأمن السيبراني وإجراءاته دورياً.

٥- يجب التأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة بشكل دوري عن طريق استخدام الأدوات المناسبة مثل:

١-٥ أنشطة تقييم مخاطر الأمن السيبراني.

٢-٥ أنشطة إدارة الثغرات.

٣-٥ أنشطة اختبار الاختراقات.

٤-٥ المراجعة الأمنية للشفرة المصدرية.

٥-٥ مراجعة معايير الأمن السيبراني.

٦-٥ مراجعة الصلاحيات على النظام والشبكة.

٧-٥ مراجعة سجلات الأمن السيبراني وحوادثه.

٦- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر نحو الالتزام بتطبيق ضوابط ومعايير الأمن السيبراني.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢. سياسة الإعدادات والتحصين

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية وتحصين وضبط إعدادات الأصول المعلوماتية والتقنية والتطبيقات الخاصة بجامعة الملك فيصل لمقاومة الهجمات السيبرانية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٦-٢-٢ والضابط رقم ١-٦-٣-٥ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة عن الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية والتطبيقات الخاصة بجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- يجب تحديد جميع الأصول المعلوماتية والتقنية المستخدمة داخل الجامعة وكذلك التطبيقات والبرمجيات المعتمدة والتأكد من توفير معايير تقنية أمنية (Technical Security Standards) لها.

٢- يجب تطوير وتوثيق واعتماد المعايير التقنية الأمنية الخاصة بجميع الأصول المعلوماتية والتقنية والتطبيقات والبرمجيات المصرح بها داخل الجامعة.

٣- يجب تحصين وضبط إعدادات أجهزة الحاسب الآلي، والأنظمة، والتطبيقات، وأجهزة الشبكات، والأجهزة الأمنية الخاصة بالجامعة بما يتوافق مع المعايير التقنية الأمنية المعتمدة لمقاومة الهجمات السيبرانية.

٤- يجب استخدام إحدى الطرق التالية لتطوير المعايير الأمنية التقنية:

٤-١ دليل الإعدادات والتحصين (Security Configuration Guidance) الخاص بالمُورد وذلك وفقاً للسياسات والإجراءات التنظيمية الخاصة بالجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات الدولية في هذا المجال.

٤-٢ دليل الإعدادات والتحصين من مصادر موثوقة ومتوافقة مع المعايير المصنعية، مثل: مركز أمن الإنترنت (CIS)، ومعهد الأمن والشبكات وإدارة النظم (SANS)، والمعهد الوطني للمعايير والتقنية (NIST)، ووكالة أنظمة معلومات الدفاع (DISA)، ودليل التطبيق الفني الأمني (STIG)، وغيرها.

٤-٣ تطوير معايير أمنية تقنية خاصة بالجامعة بما يتناسب مع طبيعة الأعمال وبما يتوافق مع دليل الإعدادات والتحصين الخاص بالمورد والمعايير المصنعية.

٥- يجب أن تغطي الضوابط الخاصة بالمعايير التقنية الأمنية بحد أدنى ما يلي:

٥-١ إيقاف أو تغيير الحسابات المصنعية والافتراضية.

٥-٢ منع تثبيت البرمجيات غير المرغوب بها.

٥-٣ تعطيل منافذ الشبكة غير المستخدمة.

٥-٤ تعطيل الخدمات غير المستخدمة.

٥-٥ تقييد استخدام وسائط الحفظ والتخزين الخارجي.

٥-٦ تغيير الإعدادات الافتراضية التي قد تُستغل في الهجمات السيبرانية.

٦- يجب مراجعة الإعدادات والتحصين والتأكد من تطبيقها في الحالات التالية:

٦-١ مراجعة الإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.

٦-٢ مراجعة الإعدادات والتحصين قبل إطلاق وتدشين المشاريع والتغييرات المتعلقة بالأصول المعلوماتية والتقنية.

٦-٣ مراجعة الإعدادات والتحصين قبل إطلاق وتدشين التطبيقات.

٦-٤ قبل إجراء التغيرات يجب دراسة تأثير التغيير على كافة جوانب الأمن السيبراني، ويجب كذلك إخطار إدارة الأمن السيبراني قبل تنفيذ أو إجراء أي تغيير.

٧- يجب اعتماد صورة (Image) لإعدادات وتحصين الأصول المعلوماتية والتقنية الخاصة بالجامعة وفقاً للمعايير التقنية الأمنية وحفظها في مكان آمن.

٨- يجب استخدام صورة (Image) معتمدة في تثبيت أو تحديث الأصول المعلوماتية والتقنية.

٩- يجب توفير التقنيات اللازمة لإدارة الإعدادات والتحصين مركزياً والتأكد من إمكانية تطبيق أو تحديث الإعدادات والتحصين تلقائياً لكافة الأصول المعلوماتية والتقنية في مواعيد زمنية محددة ومخطط لها.

١٠- يجب توفير نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة المحتوى الأمني (Security Content Automation Protocol "SCAP") للتأكد من أن الإعدادات متوافقة مع المعايير التقنية الأمنية المعتمدة ومطبقة بشكل كامل، كما يجب الإبلاغ عن أي تغييرات غير مصرّح بها.

١١- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الإعدادات والتحصين.

١٢- يجب مراجعة متطلبات الأمن السيبراني المتعلقة بالإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات الخاصة بالجامعة سنوياً أو في حالة حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

١٣- تضمين مخاطر الأمن السيبراني في سياسة الاستخدام المقبول Acceptable Use policy.

١٤- عند ترسية العقود يجب إعطاء الأولية للشركات الحاصلة على شهادات تثبت توافق معايير الأمن السيبراني لديها مع معايير الجامعة وكذلك معايير وضوابط وسياسات الهية الوطنية للأمن السيبراني.

الأدوار والمسؤوليات

راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .

- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٣. سياسة الحماية من البرمجيات الضارة

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة بجامعة الملك فيصل من تهديدات البرمجيات الضارة وتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والخوادم الخاصة بجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- البنود العامة

١-١ يجب على إدارة الأمن السيبراني تحديد تقنيات وآليات الحماية الحديثة والمتقدمة وتوفيرها والتأكد من موثوقيتها.

٢-١ يجب تطبيق تقنيات وآليات الحماية لحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم من البرمجيات الضارة (Malware) وإدارتها بشكل آمن.

٣-١ يجب التأكد من أن تقنيات وآليات الحماية قادرة على اكتشاف جميع أنواع البرمجيات الضارة المعروفة وإزالتها، مثل الفيروسات (Virus)، وأحصنة طروادة (Trojan Horse)، والديدان (Worms)، وبرمجيات التجسس (Spyware)، وبرمجيات الإعلانات المتسللة (Adware)، ومجموعة الجذر (Root Kits).

٤-١ قبل اختيار تقنيات وآليات الحماية فإنه يجب التأكد من ملاءمتها لأنظمة التشغيل الخاصة بالجامعة مثل أنظمة ويندوز (Windows) وأنظمة يونكس (UNIX) وأنظمة لينكس (Linux) ونظام ماك (Mac) وغيرها.

٥-١ في حال تسبب تحديث تقنيات الحماية بضرر للأنظمة أو متطلبات الأعمال فإنه يجب التأكد من أن تقنيات الحماية قابلة للاسترجاع إلى النسخة السابقة.

٦-١ يجب تقييد صلاحيات تعطيل التثبيت أو إلغائه أو تغيير إعدادات تقنيات الحماية من البرمجيات الضارة ومنحها لمشرفي نظام الحماية فقط.

٢- إعدادات تقنيات وآليات الحماية من البرمجيات الضارة

٢-١ يجب ضبط إعدادات تقنيات الحماية وآلياتها وفقاً للمعايير التقنية الأمنية المعتمدة لدى الجامعة مع الأخذ بالاعتبار إرشادات المورد وتوصياته.

٢-٢ يجب ضبط إعدادات برنامج مكافحة الفيروسات على خوادم البريد الإلكتروني لفحص جميع رسائل البريد الإلكتروني الواردة والصادرة.

٢-٣ لا يُسمح للأشخاص التابعين لأطراف خارجية بالاتصال بالشبكة أو الشبكة اللاسلكية للجامعة دون تحديث برنامج مكافحة الفيروسات وضبط الإعدادات المناسبة.

٢-٤ يجب ضمان توافر خوادم برامج الحماية من البرمجيات الضارة .

٢-٥ يجب منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت المعروفة باستضافتها لبرمجيات ضارة وذلك باستخدام آلية تصفية محتوى الويب (Filtering Web Content).

٢-٦ يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع تقنيات وآليات الحماية من البرمجيات الضارة.

٢-٧ يجب ضبط إعدادات تقنيات الحماية من البرمجيات الضارة للقيام بعمليات التحقق من المحتوى المشبوه في مصادر معزولة مثل صندوق الفحص (Sandbox).

٢-٨ يجب القيام بعمليات مسح دورية لأجهزة المستخدمين والخوادم والتأكد من سلامتها من البرمجيات الضارة.

٢-٩ يجب تحديث تقنيات الحماية من البرمجيات الضارة تلقائياً عند توفر إصدارات جديدة من المورد، مع الأخذ بالاعتبار سياسة إدارة التحديثات والإصلاحات.

٢-١٠ يجب توفير تقنيات حماية البريد الإلكتروني وتصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، والتي تستخدم عادةً الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وتطبيقها وإداراتها بشكل آمن.

٢-١١ يجب ضبط إعدادات تقنيات الحماية بالسماح لقائمة محددة فقط من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة. (CSCC-2-3-1-1)

٢-١٢ يجب حماية الخوادم الخاصة بالأنظمة الحساسة عن طريق تقنيات حماية الأجهزة الطرفية المعتمدة لدى الجامعة (End-point Protection). (CSCC-2-3-1-2)

٢-١٣ يجب العمل على إدارة تقنيات الحماية من البرمجيات الضارة مركزياً ومراقبتها باستمرار.

٢-١٤ يجب على إدارة الأمن السيبراني إعداد تقارير دورية حول حالة الحماية من البرمجيات الضارة يوضح فيها عدد الأجهزة والخوادم المرتبطة بتقنيات الحماية وحالتها (مثل: محدثة، أو غير محدثة، أو غير متصلة، إلخ)، ورفعها إلى المسؤول على إدارة الأمن السيبراني .

٣- متطلبات أخرى

٣-١ يجب على إدارة الأمن السيبراني التأكد من توافر الوعي الأمني اللازم لدى جميع العاملين للتعامل مع البرمجيات الضارة والتقليل من مخاطرها.

٣-٢ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والخوادم من البرمجيات الضارة.

٣-٣ يجب مراجعة متطلبات الأمن السيبراني لحماية أجهزة المستخدمين والخوادم الخاصة بالجامعة دورياً.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٤. سياسة أمن الخوادم

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالخوادم (Servers) الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الخوادم الخاصة بجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- البنود العامة

١-١ يجب تحديد جميع الخوادم الخاصة بالجامعة وتوثيقها والتأكد من أن برمجيات الخوادم محدثة ومعتمدة.

٢-١ يجب تطوير وتطبيق معايير تقنية أمنية (Technical Security Standards) للخوادم المستخدمة داخل الجامعة باستخدام أفضل المعايير الدولية.

٣-١ يجب ضبط إعدادات الخوادم وفقاً للمعايير التقنية الأمنية المعتمدة قبل تشغيل الخوادم في بيئة الإنتاج.

٤-١ يجب توفير الحماية اللازمة لجميع الخوادم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة.

٥-١ يجب عمل نسخ احتياطية منتظمة للخوادم وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في الجامعة لضمان إمكانية استعادتها في حال تعرّضها لتلف أو حادث غير مقصود. مع ضرورة عمل نسخ احتياطية يومياً للأنظمة الحساسة.

٦-١ يجب تحديث برمجيات الخوادم بما في ذلك أنظمة التشغيل وبرامج التطبيقات وتزويدها بأحدث حزم التحديثات والإصلاحات الأمنية وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في الجامعة.

٢- إعدادات الخوادم

١-٢ يجب اعتماد صورة (Image) لإعدادات وتحصين أنظمة تشغيل الخوادم الخاصة بالجامعة وحفظها في مكان آمن وفقاً للمعايير التقنية الأمنية المعتمدة.

٢-٢ يجب استخدام صورة (Image) معتمدة لتثبيت أنظمة تشغيل الخوادم أو تحديثها.

٣-٢ يجب اعتماد إعدادات وتحصين الخوادم، ومراجعتها وتحديثها دورياً وكل ستة أشهر على الأقل بالنسبة لخوادم الأنظمة الحساسة (CSCC-2-3-1-6).

٣- الوصول والإدارة

٣-١ يجب تقييد الوصول إلى الخوادم الخاصة بالجامعة بحيث يكون الوصول متاحاً للمستخدمين المصرح لهم وعند الحاجة فقط.

٣-٢ يجب تقييد الدخول إلى الخوادم وحصره على حسابات مشرفي الأنظمة ومراجعة الحسابات والصلاحيات الممنوحة للمشرفين بشكل دوري.

٣-٣ يجب تقييد الوصول إلى الخوادم الخاصة بالأنظمة الحساسة وحصره على الفريق التقني ذي الصلاحيات الهامة وذلك عن طريق أجهزة حاسب (Workstations)، كما يجب عزل هذه الأجهزة في شبكة خاصة لإدارة الأنظمة (Management Network)، ومنع ارتباطها بأي شبكة أو خدمة أخرى (مثل خدمة البريد الإلكتروني والإنترنت).

٣-٤ يجب استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول إلى الخوادم الخاصة بالأنظمة الحساسة (CSCC-3-1-2-2).

٣-٥ يجب إيقاف الحسابات المصنعية والافتراضية أو تغييرها، وإيقاف الخدمات غير المستخدمة، ومنافذ الشبكة غير المستخدمة في نظام التشغيل (Operating System).

٣-٦ يجب حماية البيانات المخزنة على الخوادم وتشفيرها بالتوافق مع ضوابط التشفير المعتمدة بناءً على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة. (ECC-2-8-3-3).

٤- حماية الخوادم

٤-١ يجب أن تُمنَع الخوادم غير المحدّثة أو غير الموثوقة من الاتصال بشبكة الجامعة ووضعها في شبكة معزولة لأخذ التحديثات اللازمة لتقليل المخاطر السيبرانية ذات العلاقة والتي قد تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات.

٤-٢ يجب استخدام تقنيات وآليات الحماية الحديثة والمتقدمة للحماية من الفيروسات (Virus) والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) وإدارتها بشكل آمن.

٤-٣ يجب السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة (CSCC-2-3-1-1).

٤-٤ يجب تقييد استخدام وسائط التخزين الخارجية على الخوادم، ويجب الحصول على إذن مسبق من إدارة الأمن السيبراني قبل استخدامها، والتأكد من استخدامها بشكل آمن.

٤-٥ يجب تثبيت الخوادم في المنطقة المناسبة من مخطط/هيكل الشبكة حسب المتطلبات التشغيلية والتشريعية لها لضمان إدارتها وتطبيق الحماية اللازمة عليها بشكل فعّال.

٥- المتطلبات التشغيلية لإدارة الخوادم

٥-١ يجب إدارة الخوادم مركزياً في الجامعة لكشف المخاطر بصورة أسرع، وتسهيل إدارة ومراقبة الخوادم مثل تقييد الوصول وتثبيت حزم التحديثات وغيرها.

٥-٢ يجب توفير الحماية اللازمة للخوادم التي تعمل في بيئة الأنظمة الافتراضية (Environment Virtual) وإدارتها بشكل آمن حسب تقييم المخاطر.

٥-٣ يجب ضبط إعدادات الخوادم وتفعيل إرسال سجلات الأحداث إلى نظام السجلات والمراقبة (SIEM) وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

٥-٤ يجب مزامنة توقيت جميع الخوادم مركزياً (Clock Synchronization) من مصدر دقيق وموثوق ومعتمد.

٥-٥ يجب توفير المتطلبات اللازمة لتشغيل الخوادم بشكل آمن وملائم، مثل توفير بيئة مناسبة وآمنة وتقييد الوصول المادي إلى منطقة الخوادم للعاملين المصرح لهم فقط ومراقبته.

٥-٦ يجب على قسم الشبكات ونظم التشغيل بعمادة تقنية المعلومات مراقبة مكونات الخوادم التشغيلية والتأكد من فعالية أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحو ذلك.

٦- إدارة الثغرات واختبار الاختراق

٦-١ يجب فحص الخوادم واكتشاف الثغرات الموجودة فيها ومعالجتها بناءً على تصنيف الثغرات المكتشفة والمخاطر السيبرانية المترتبة عليها دورياً ومرة واحدة شهرياً على الأقل بالنسبة لخوادم الأنظمة الحساسة (CSCC-2-9-1-2).

٦-٢ يجب تنفيذ عمليات اختبار الاختراق على الخوادم دورياً وكل ١٢ شهر على الأقل على خوادم الأنظمة الحساسة (CSCC-2-10-2).

٦-٣ يجب تثبيت حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات ورفع مستوى كفاءة الخوادم وأمنها، حسب سياسة إدارة التحديثات والإصلاحات.

٧- الحماية المادية والبيئية للخوادم

٧-١ يجب رصد ومراقبة الدخول والخروج من مرافق الجامعة (على سبيل المثال الأبواب والأقفال).

٧-٢ يجب رصد ومراقبة العوامل البيئية كالتدفئة وتكييف الهواء والدخان وأجهزة إنذار الحريق وأنظمة إخماد الحرائق.

٧-٣ يجب الالتزام بوضع الضوابط الأمنية المادية المناسبة (مثل كاميرات المراقبة داخل وخارج مركز بيانات الجامعة، وحراس الأمن، وتأمين الكابلات، وغيرها).

٨- متطلبات أخرى

٨-١ يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لحماية الخوادم.

٨-٢ يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة الخوادم سنوياً على الأقل أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٥. سياسة أمن الشبكات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بأمن الشبكات الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الشبكات التقنية الخاصة بجامعة الملك فيصل وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- البنود العامة

١-١ تحديد وتوثيق جميع أجهزة الشبكة داخل الجامعة والتأكد من أن جميع الأجهزة محدثة ومعتمدة.

١-٢ توثيق واعتماد معايير تقنية أمنية (Technical Security Standards) لجميع أجهزة الشبكة المستخدمة داخل الجامعة.

١-٣ إدارة صلاحيات الدخول إلى الشبكات الخاصة بالجامعة وفقاً لسياسة إدارة هويات الدخول والصلاحيات، بحيث يكون الاتصال بالشبكة متوفراً عند الحاجة ومتاحاً للمستخدمين المصرح لهم فقط.

٢- متطلبات الوصول إلى الشبكة

٢-١ تطوير واعتماد إجراءات خاصة بمنح وإلغاء صلاحيات الدخول إلى الشبكة وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات الخاصة بالجامعة.

٢-٢ للحصول على صلاحية الدخول إلى الشبكة فإنه يجب على المستخدم تقديم طلب إلى عمادة تقنية المعلومات يوضح فيه نوع الطلب وفترة صلاحيته ومبرراته.

٢-٣ في حال إضافة أو التعديل على قوائم جدار الحماية فإنه يجب على مسؤول الشبكة توثيق متطلبات الأعمال ومعلومات الطلب في نظام جدار الحماية.

٢-٤ يجب استخدام اسم المستخدم وكلمة المرور للدخول إلى الشبكة الخاصة بالجامعة وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

٢-٥ مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) دورياً وكل ستة أشهر على الأقل للأنظمة الحساسة. (CSCC-2-4-1-2)

٢-٦ توفير الحماية اللازمة عند تصفح الإنترنت والاتصال به وتقييد الدخول إلى المواقع الإلكترونية المشبوهة ومواقع مشاركة تخزين الملفات ومواقع الدخول عن بعد.

٢-٧ عدم ربط الشبكة اللاسلكية بالشبكة الداخلية للجامعة إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك، والتعامل معها بما يضمن حماية الأصول التقنية الخاصة وسرية البيانات وسلامتها، وحماية النظم والتطبيقات المتصلة بأنظمة الجامعة.

٢-٨ يُمنع ربط الأنظمة الحساسة بالشبكة اللاسلكية للجامعة.

٢-٩ يجب توفير التقنيات اللازمة لوضع القيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.

٢-١٠ يمنع الربط المباشر لأي جهاز بالشبكة المحلية للأنظمة الحساسة قبل فحصه والتأكد من توافر عناصر الحماية المحققة للمستوى المقبول للأنظمة الحساسة (CSCC-2-4-1-3).

٣- متطلبات وصول الأطراف الخارجية إلى الشبكة

٣-١ يخضع منح صلاحية وصول الأطراف الخارجية لشبكة الجامعة إلى متطلبات الأمن السيبراني المشار إليها في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية.

٣-٢ استخدام تقنيات تشفير ومصادقة آمنة لنقل البيانات من الأطراف الخارجية وإليها.

٣-٣ تحديد مدة زمنية معينة للأطراف الخارجية للدخول إلى شبكة الجامعة.

٣-٤ مراجعة صلاحيات المستخدمين والأطراف الخارجية دورياً وذلك وفقًا لسياسات الأمن السيبراني المعتمدة في الجامعة.

٤- حماية الشبكات

٤-١ يجب عزل وتقسيم الشبكات مادياً ومنطقياً باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth). (ECC-2-5-3-1)

٤-٢ تطبيق العزل المنطقي لشبكة الأنظمة الحساسة (VLAN).

٤-٣ تطبيق العزل المنطقي بين شبكة بيئة الإنتاج وشبكة بيئة الاختبار والشبكات الأخرى.

٤-٤ يمنع ربط الأنظمة الحساسة بالإنترنت في حال كانت هذه الأنظمة تقدم خدمة داخلية للجامعة. ولا توجد هناك حاجة ضرورية جداً للدخول على الخدمة من خارج جامعة الملك فيصل (CSCC-2-4-1-6).

٤-٥ تطبيق العزل المنطقي بين شبكة الاتصالات الهاتفية عبر الإنترنت (Voice Over IP "VOIP") وشبكة البيانات.

٤-٦ تقييد استخدام منافذ الشبكة المادية في جميع مرافق الجامعة وذلك باستخدام خاصية حماية المنافذ (Port Security) أو تقنية التحقق من الأجهزة (Port-Based Authentication) لحماية الشبكة من احتمالية ربط أجهزة غير مصرح بها أو أجهزة مشبوهة دون أن يتم كشفها.

٤-٧ توفير أنظمة الحماية في قناة تصفح الإنترنت للحماية من التهديدات المتقدمة المستمرة (APT Protection) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المتوقعة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.

٤-٨ يمنع اتصال الشبكة الداخلية بالإنترنت مباشرةً، ويكون الاتصال عن طريق استخدام موزع اتصالات الإنترنت (Proxy) لتحليل وتصفية البيانات المنتقلة من وإلى شبكة الجامعة.

٤-٩ ضبط إعدادات قوائم جدار الحماية بحيث تُحظر جميع أنواع الاتصالات بين أجزاء الشبكة تلقائياً (Explicitly)، ويتم إتاحة قوائم جدار الحماية بناءً على طلب المستخدم ومتطلبات الأعمال.

٤-١٠ يجب توفير التقنيات اللازمة لأمن نظام أسماء النطاقات (DNS).

٤-١١ يجب توفير أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems) على جميع أجزاء الشبكة وتحديثها دورياً.

٤-١٢ يجب توفير أنظمة الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT) على شبكة الأنظمة الحساسة.

٤-١٣ يجب تطبيق آليات حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT) والبرمجيات الضارة غير المعروفة مسبقاً وإدارتها بشكل آمن. (ECC-2-5-3-8)

٤-١٤ يجب توفير أنظمة الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") على الأنظمة الخارجية الحساسة. (CSCC-2-4-1-8)

٥- الأمن المادي والبيئي

٥-١ يجب حفظ أجهزة الشبكات في بيئة آمنة وملائمة، والتأكد من ضبط درجة الحرارة والرطوبة وكذلك وجود مصادر طاقة احتياطية مثل (Uninterruptible Power Supply "UPS").

٥-٢ يجب تقييد الدخول المادي إلى أجهزة الشبكات للمصرح لهم فقط لحفظ الأجهزة وحمايتها من السرقة أو العبث.

٥-٣ يجب حفظ سجلات الدخول ومراقبة مناطق أجهزة الشبكات الخاصة بالأنظمة الحساسة (CCTV) ومراجعتها دورياً.

٦- متطلبات أخرى

٦-١ يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لأمن الشبكات.

٦-٢ يجب مراجعة متطلبات الأمن السيبراني الخاصة بأمن الشبكات سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٦. سياسة أمن البريد الإلكتروني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية البريد الإلكتروني لجامعة الملك فيصل من المخاطر السيبرانية والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة البريد الإلكتروني الخاصة بجامعة الملك فيصل وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- يجب توفير تقنيات حديثة لحماية البريد الإلكتروني وتحليل وتصفية (Filtering) رسائل البريد الإلكتروني وحظر الرسائل المشبوهة، مثل الرسائل الاقتحامية (Spam Emails) ورسائل التصيّد الإلكتروني (Phishing Emails).

٢- يجب أن تستخدم أنظمة البريد الإلكتروني أرقام تعريف المستخدم وكلمات المرور مرتبطة وذلك لضمان عزل اتصالات المستخدمين المختلفين.

٣- يجب توفير التقنيات اللازمة لتشفير البريد الإلكتروني الذي يحتوي على معلومات مصنفة.

٤- يجب تطبيق خاصية التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).

٥- يجب أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دورياً.

٦- يجب تحديد مسؤولية البريد الإلكتروني للحسابات العامة والمشتركة (Generic Account)

٧- يجب توفير تقنيات الحماية اللازمة من الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Protection) على خوادم البريد الإلكتروني والتأكد من فحص الرسائل قبل وصولها لصندوق بريد المستخدم.

٨- يجب توثيق مجال البريد الإلكتروني للجامعة عن طريق استخدام الوسائل اللازمة مثل طريقة إطار سياسة المرسل (Sender Policy Framework) لمنع تزوير البريد الإلكتروني (Email Spoofing). كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة (Incoming message DMARC verification).

٩- يجب أن يقتصر الوصول إلى رسائل البريد الإلكتروني على طلبة ومنسوبي الجامعة.

١٠- يجب اتخاذ الإجراءات اللازمة لمنع استخدام البريد الإلكتروني للجامعة وذلك في غير أغراض العمل.

١١- يمنع وصول مسؤول النظام (System Administrator) إلى معلومات البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق.

١٢- يجب تحديد حجم مرفقات البريد الإلكتروني الصادر والوارد وسعة صندوق البريد لكل مستخدم. وكذلك العمل على الحد من إتاحة إرسال الرسائل الجماعية لعدد كبير من المستخدمين.

١٣- يجب تذييل رسائل البريد الإلكتروني المرسلة إلى خارج الجامعة وذلك من خلال إشعار إخلاء المسؤولية.

١٤- يجب تطبيق التقنيات اللازمة لحماية سرية رسائل البريد الإلكتروني وسلامتها، وتوافرها أثناء نقلها وحفظها وتشمل هذه الإجراءات استخدام تقنيات التشفير وتقنيات منع تسريب البيانات.

١٥- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام البريد الإلكتروني.

١٦- يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم (Open Mail Relay).

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٧. سياسة الاستخدام المقبول للأصول

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة جامعة الملك فيصل وأصولها، وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- البنود العامة

١-١ يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة حماية وتصنيف البيانات والمعلومات بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

١-٢ يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.

١-٣ يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

١-٤ يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.

١-٥ يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.

١-٦ يجب الالتزام بسياسة المكتب الآمن والنظيف والتأكد من خلو سطح المكتب وكذلك شاشة العرض من المعلومات المصنفة.

١-٧ يمنع الإفصاح عن أي معلومات تخص الجامعة بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.

١-٨ يُمنع نشر معلومات تخص الجامعة عبر وسائل الإعلام وشبكات التواصل الاجتماعي دون تصريح مسبق.

١-٩ يُمنع استخدام أنظمة الجامعة وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال الجامعة.

١-١٠ يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بالجامعة بما في ذلك برامج مكافحة الفيروسات وجدار الحماية والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى الجامعة.

١-١١ تحتفظ إدارة الأمن السيبراني بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.

١-١٢ يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

١-١٣ يجب ارتداء البطاقة التعريفية في جميع مرافق الجامعة.

١-١٤ يجب تبليغ إدارة الأمن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.

٢- حماية أجهزة الحاسب الآلي

٢-١ يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

٢-٢ يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من إدارة الأمن السيبراني، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

٢-٣ يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

٢-٤ يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

٢-٥ يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من عمادة تقنية المعلومات.

٢-٦ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بجامعة الملك فيصل أو أصولها.

٣- الاستخدام المقبول للإنترنت والبرمجيات

٣-١ يجب إبلاغ إدارة الأمن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها أو العكس.

٣-٢ يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

٣-٣ يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

٣-٤ يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

٣-٥ يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

٣-٦ يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول الجامعة دون الحصول على تصريح مسبق من عمادة تقنية المعلومات.

٣-٧ يُمنع استخدام شبكة الإنترنت في غير أغراض العمل بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

٣-٨ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

٣-٩ يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكة الجامعة وأنظمتها أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

٣-١٠ يُمنع استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

٣-١١ يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

٤- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

٤-١ يُمنع استخدام البريد الإلكتروني، أو الهاتف، أو الفاكس، أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

٤-٢ يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

٤-٣ يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

٤-٤ يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بالجامعة في أي موقع ليس له علاقة بالعمل.

٤-٥ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة الجامعة أو أصولها.

٤-٦ تحتفظ الجامعة بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وإدارة الأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة.

٤-٧ يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

٥- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

٥-١ يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.

٥-٢ يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

٦- استخدام كلمات المرور

٦-١ يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة الجامعة وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

٦-١ يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو عمادة تقنية المعلومات.

٦-٢ يجب تغيير كلمة المرور، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني وجميع العاملين.

الالتزام بالسياسة

يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.

- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٨. سياسة مراجعة وتدقيق الأمن السيبراني

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لمراجعة وتدقيق ضوابط الأمن السيبراني لدى جامعة الملك فيصل والتأكد من تطبيقها وأنها تعمل وفقاً للسياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيمياً على جامعة الملك فيصل.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-٨-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع ضوابط الأمن السيبراني في جامعة الملك فيصل وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- البنود العامة

١-١ يجب على إدارة الأمن السيبراني مراجعة تطبيق ضوابط الأمن السيبراني دورياً، ومراجعة مدى الالتزام بالضوابط الأساسية للأمن السيبراني (ECC:1-2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019) الصادرة من الهيئة الوطنية للأمن السيبراني.

١-٢ يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني دورياً من قبل أطراف مستقلة عن إدارة الأمن السيبراني، كما يمكن الاستعانة بأطراف خارجية مع تطبيق الإجراءات النظامية في هذا الشأن.

١-٣ يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة مرة واحدة كل ثلاث سنوات على الأقل من قبل أطراف مستقلة عن إدارة الأمن السيبراني من داخل الجامعة.

١-٤ يجب التأكد من تطبيق ضوابط الأمن السيبراني دورياً، ومرّة واحدة سنوياً على الأقل للأنظمة الحسّاسة للتأكد من مواءمتها مع الضوابط الأساسية للأمن السيبراني (ECC:1-2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019).

١-٥ يجب تحديد إجراءات مراجعة وتدقيق الأمن السيبراني وتوثيقها.

١-٦ يجب توثيق نتائج مراجعة وتدقيق الأمن السيبراني ومناقشتها مع الجهات المعنية.

١-٧ يجب عرض النتائج على اللجنة الإشرافية للأمن السيبراني في الجامعة وصاحب الصلاحية، كما يجب أن تشمل النتائج نطاق المراجعة والتدقيق، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وتقييم المخاطر وخطة معالجة الملاحظات.

٨-١ يجب اعتماد جدول المسؤوليات التالي (RACI Chart) في تنفيذ عمليات مراجعة وتدقيق الأمن السيبراني، وذلك وفقاً للجدول أدناه (جدول رقم: ٧ - مصفوفة توزيع الصلاحيات والمسؤوليات في تنفيذ عمليات مراجعة وتدقيق الأمن السيبراني).

	جهة التدقيق الخارجية	قسم التطوير والجودة بعمادة تقنية المعلومات	إدارة الأمن السيبراني	المسؤول على إدارة الأمن السيبراني	رئيس اللجنة الإشرافية للأمن السيبراني في الجامعة
مراجعة الأمن السيبراني	R	R	R	A	I
تدقيق الأمن السيبراني	R	R	I	I	A
تنفيذ الإجراءات التصحيحية	C / I	C / I	R	R	A

R: Responsible - المُنفذ

A: Accountable - المسؤول

C: Consulted - المُستشار

I: Informed - المُطّلع

٢- متطلبات أخرى

٢-١ يجب أن تتخذ إدارة الأمن السيبراني إجراءات استباقية وتصحيحية خاصة بنتائج المراجعة والتدقيق.

٢-٢ يجب على إدارة الأمن السيبراني تحديد العوامل التي أدّت إلى هذه الملاحظات وتحليلها ومعرفة أسبابها والحد من تكرارها.

٢-٣ يجب مراجعة سياسة مراجعة وتدقيق الأمن السيبراني سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** قسم التطوير والجودة بعمادة تقنية المعلومات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.

- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٩. سياسة إدارة هويات الدخول والصلاحيات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة هويات الدخول والصلاحيات على الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، وذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- إدارة هويات الدخول والصلاحيات (Identity and Access Management)

١-١ إدارة الصلاحيات

١-١-١ توثيق واعتماد إجراء لإدارة الوصول يوضح آلية منح صلاحيات الوصول للأصول المعلوماتية والتقنية وتعديلها وإلغائها في الجامعة، ومراقبة هذه الآلية والتأكد من تطبيقها.

١-١-٢ إنشاء هويات المستخدمين (User Identities) وفقاً للمتطلبات التشريعية والتنظيمية الخاصة بالجامعة.

١-١-٣ التحقق من هوية المستخدم (Authentication) والتحقق من صحتها قبل منح المستخدم صلاحية الوصول إلى الأصول المعلوماتية والتقنية.

١-١-٤ توثيق واعتماد مصفوفة (Matrix) لإدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:

١-١-٤-١ مبدأ الحاجة إلى المعرفة والاستخدام (Need-to-Know and Need-to-Use).

١-١-٤-٢ مبدأ فصل المهام (Segregation of Duties).

١-١-٤-٣ مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege).

١-١-٥ تطبيق ضوابط التحقّق والصلاحيات على جميع الأصول التقنية والمعلوماتية في الجامعة من خلال نظام مركزي آلي للتحكّم في الوصول، مثل بروتوكول النفاذ إلى الدليل البسيط (Lightweight Directory Access Protocol "LDAP").

١-١-٦ منع استخدام الحسابات المشتركة (Generic User) للوصول إلى الأصول المعلوماتية والتقنية الخاصة بالجامعة.

١-١-٧ ضبط إعدادات الأنظمة ليتم إغلاقها تلقائياً بعد فترة زمنية محدّدة (Session Timeout)، (يوصى ألا تتجاوز الفترة ١٥ دقيقة).

١-١-٨ تعطيل حسابات المستخدمين غير المستخدمة خلال فترة زمنية محدّدة (يوصى ألا تتجاوز الفترة ٩٠ يوماً).

١-١-٩ ضبط إعدادات جميع أنظمة إدارة الهويات والوصول لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

١-١-١٠ عدم منح المستخدمين صلاحيات الوصول أو التعامل المباشر مع قواعد البيانات للأنظمة الحساسة، حيث يكون ذلك من خلال التطبيقات فقط، ويستثنى من ذلك مشرفي قواعد البيانات (Database Administrators). [CSCC-2-2-1-7]

١-١-١١ توثيق واعتماد إجراءات واضحة للتعامل مع حسابات الخدمات (Service Account) والتأكد من إدارتها بشكل آمن ما بين التطبيقات والأنظمة، وتعطيل الدخول البشري التفاعلي (Interactive Login) من خلالها. (CSCC-2-2-1-7)

١-٢ منح حق الدخول

١-٢-١ متطلبات حق الدخول لحسابات المستخدمين

١-٢-١-١ منح صلاحية الدخول بناءً على طلب المستخدم من خلال نموذج أو عن طريق النظام المعتمد من قبل مديره المباشر ومالك النظام (System Owner) يُحدّد فيه اسم النظام ونوع الطلب والصلاحية ومدتها (في حال كانت صلاحية الدخول مؤقتة).

١-٢-١-٢ منح المستخدم حق الوصول إلى الأصول المعلوماتية والتقنية الخاصة بالجامعة بما يتوافق مع الأدوار والمسؤوليات الخاصة به.

١-٢-١-٣ اتباع آلية موحدة لإنشاء هويات المستخدمين بطريقة تتيح تتبع النشاطات التي يتم أداؤها باستخدام "هوية المستخدم" (User ID) وربطها مع المستخدم، مثل كتابة <الحرف الأول من الاسم الأول> نقطة <الاسم الأخير>، أو كتابة رقم الموظف المعرف مسبقاً لدى الجهة/الجهات المسؤولة عن الموارد البشرية بالجامعة.

١-٢-١-٤ تعطيل إمكانية تسجيل دخول المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت (Concurrent Logins).

١-٢-٢ متطلبات حق الوصول للحسابات الهامة والحسّاسة

بالإضافة إلى الضوابط المذكورة في قسم متطلبات حق الوصول لحسابات المستخدمين، يجب أن تُطبَق الضوابط المُوضّحة أدناه على الحسابات ذات الصلاحيات الهامة والحسّاسة:

١-٢-٢-١ تعيين حق وصول مستخدم فردي للمستخدمين الذين يطلبون الصلاحيات الهامة والحسّاسة (Administrator Privilege) ومنحهم هذا الحق بناءً على مهامهم الوظيفية، مع الأخذ بالاعتبار مبدأ فصل المهام.

٢-٢-٢-١ يجب تفعيل سجل كلمة المرور (Password History) لتتبع عدد كلمات المرور التي تم تغييرها.

٣-٢-٢-١ تغيير أسماء الحسابات الافتراضية، وخصوصاً الحسابات الحاصلة على صلاحيات هامة وحسّاسة مثل "الحساب الرئيسي" (Root) وحساب "مدير النظام" (Admin) وحساب "مُعرّف النظام الفريد" (Sys id).

٤-٢-٢-١ منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في العمليات التشغيلية اليومية.

٥-٢-٢-١ التحقّق من حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة على الأصول التقنية والمعلوماتية من خلال آلية التحقّق من الهوية متعدد العناصر (Multi-Factor Authentication "MFA") باستخدام طريقتين على الأقل من الطرق التالية:

- المعرفة (شيء يعرفه المستخدم "مثل كلمة المرور").
- الحيازة (شيء يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها "One-Time-Password").
- الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصة الإصبع").

٦-٢-٢-١ يجب أن يتطلب الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها استخدام التحقق من الهوية متعدد العناصر (MFA) لجميع المستخدمين.

٣-٢-١ الدخول عن بُعد إلى شبكة الجامعة

١-٣-٢-١ منح صلاحية الدخول عن بعد للأصول المعلوماتية والتقنية بعد الحصول على إذن مسبق من إدارة الأمن السيبراني وتقييد الدخول باستخدام التحقق من الهوية متعدد العناصر (MFA).

٢-٣-٢-١ حفظ سجلات الأحداث المتعلقة بجميع جلسات الدخول عن بُعد الخاصة ومراقبتها حسب حساسية الأصول المعلوماتية والتقنية.

٣-١ إلغاء وتغيير حق الوصول

١-٣-١ يجب على الجهة/الجهات المسؤولة عن الموارد البشرية بالجامعة تبليغ عمادة تقنية المعلومات لاتخاذ الإجراء اللازم عند انتقال المستخدم أو تغيير مهامه أو إنهاء/انتهاء العلاقة الوظيفية بين المستخدم وجامعة الملك فيصل. وتقوم عمادة تقنية المعلومات بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمستخدم بناءً على مهامه الوظيفية الجديدة.

٢-٣-١ في حال تم إيقاف صلاحيات المستخدم، يمنع حذف سجلات الأحداث الخاصة بالمستخدم ويتم حفظها وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

٢- مراجعة هويات الدخول والصلاحيات

٢-١ مراجعة هويات الدخول (User IDs) والتحقق من صلاحية الوصول إلى الأصول المعلوماتية والتقنية وفقاً للمهام الوظيفية للمستخدم بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة هويات الدخول على الأنظمة الحساسة مرة واحدة كل ثلاثة أشهر على الأقل.

٢-٢ يجب تسجيل وتوثيق جميع محاولات الوصول الفاشلة والناجحة ومراجعتها دورياً.

٣- إدارة كلمات المرور

٣-١ تطبيق سياسة آمنة لكلمة المرور ذات معايير عالية لجميع الحسابات داخل الجامعة، ويتضمّن الجدول أدناه (جدول رقم: ٨ - ضوابط كلمات المرور) أمثلة على ضوابط كلمات المرور لكل مستخدم:

ضوابط كلمات المرور	جميع المستخدمين (All Users)	حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة (Privileged Users)	حسابات الخدمات (Service Account)
الحدّ الأدنى لعدد أحرف كلمة المرور	٨ أحرف أو أرقام أو رموز	١٢ حرفاً أو رقماً أو رمزاً	٨ أحرف أو أرقام أو رموز
سجل كلمة المرور	تذكّر ٥ كلمات مرور	تذكّر ٥ كلمات مرور	تذكّر ٥ كلمات مرور
الحد الأعلى لعمر كلمة المرور	٦ شهور	٤٥ يوماً	٤٥ يوماً
مدى تعقيد كلمة المرور	مُفعّل	مُفعّل	مُفعّل
مثال على تعقيد كلمة المرور	D_dyW5$_	R@rS%7qY#b!u	r?M4d5V=
مدة إغلاق الحساب	١٠ دقيقة أو حتى يقوم النظام بفك الإغلاق	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق
حد إغلاق الحساب	٢٥ محاولات غير صحيحة لتسجيل الدخول	٥ محاولات غير صحيحة لتسجيل الدخول	لا توجد محاولات
إعادة ضبط عداد إغلاق الحساب بعد مرور فترة معينة	٥ دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	٣٠ دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	لا يوجد
استخدام التحقق متعدد العناصر	مُفعل على الدخول عن بعد فقط	مُفعل	غير مُفعل

٣-٢ معايير كلمات المرور

٣-٢-١ يجب أن تتضمّن كلمة المرور (٨) أحرف على الأقل.

٣-٢-٢ يجب أن تكون كلمة المرور معقّدة (Complex Password) وتتضمّن ثلاثة رموز من الرموز التالية على الأقل:

٣-٢-٢-١ أحرف كبيرة (Upper Case Letters).

٣-٢-٢-٢ أحرف صغيرة (Lower Case Letters).

٣-٢-٢-٣ أرقام (١٢٣٥).

٣-٢-٢-٤ رموز خاصّة (@*%#).

٣-٢-٣ يجب إشعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية.

٣-٢-٤ يجب ضبط إعدادات كافة الأصول المعلوماتية والتقنية لطلب تغيير كلمة المرور المؤقتة عند تسجيل المستخدم الدخول لأول مرة.

٣-٢-٥ يجب تغيير جميع كلمات المرور الافتراضية لجميع الأصول المعلوماتية والتقنية قبل تثبيتها في بيئة الإنتاج.

٣-٢-٦ يجب تغيير كلمات مرور السلاسل النصية (Community String) الافتراضية (مثل: «Public» و«Private» و«System») الخاصة ببروتوكول إدارة الشبكة البسيط (SNMP)، ويجب أن تكون مختلفة عن كلمات المرور المستخدمة لتسجيل الدخول في الأصول التقنية المعنية.

٣-٣ حماية كلمات المرور

٣-٣-١ يجب تشفير جميع كلمات المرور للأصول المعلوماتية والتقنية الخاصة بالجامعة بصيغة غير قابلة للقراءة أثناء إدخالها ونقلها وتخزينها وذلك وفقاً لسياسة التشفير.

٣-٣-٢ يجب إخفاء (Mask) كلمة المرور عند إدخالها على الشاشة.

٣-٣-٣ يجب تعطيل خاصية "تذكّر كلمة المرور" (Remember Password) على الأنظمة والتطبيقات الخاصة بالجامعة.

٣-٣-٤ منع استخدام الكلمات المعروفة (Dictionary) في كلمة المرور كما هي.

٣-٣-٥ يجب تسليم كلمة المرور الخاصة بالمستخدم بطريقة آمنة وموثوقة.

٣-٣-٦ إذا طلب المستخدم إعادة تعيين كلمة المرور عن طريق الهاتف أو الإنترنت أو أي وسيلة أخرى، فلا بد من التحقّق من هوية المستخدم قبل إعادة تعيين كلمة المرور.

٣-٣-٧ يجب حماية كلمات المرور الخاصة بحسابات الخدمة والحسابات ذات الصلاحيات الهامة والحسّاسة وتخزينها بشكل آمن في موقع مناسب (داخل ظرف مغلق ومختوم وحفظه في خزنة) أو استخدام التقنيات الخاصة بحفظ وإدارة الصلاحيات الهامة والحسّاسة (Privilege Access Management Solution).

٤- متطلبات أخرى

٤-١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة هويات الدخول والصلاحيات.

٤-٢ يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات دورياً.

٤-٣ يجب مراجعة هذه السياسة سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** الأقسام ذات الصلة بعمادة تقنية المعلومات، والجهة/الجهات المسؤولة عن الموارد البشرية بالجامعة، وإدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٠. سياسة الأمن السيبراني للموارد البشرية

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في جامعة الملك فيصل تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة الخاصة بجامعة الملك فيصل وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

البنود العامة

١-١ يجب تحديد متطلبات الأمن السيبراني المتعلقة بالعاملين.

٢-١ يجب أن يشغل الوظائف ذات العلاقة بالأنظمة الحساسة في الجامعة مواطنون من ذوي الكفاءة اللازمة.

٣-١ يجب تنفيذ ضوابط الأمن السيبراني الخاصة بالموارد البشرية خلال دورة حياة عمل الموظف (Lifecycle) في الجامعة والتي تشمل المراحل التالية:

- قبل التوظيف
- خلال فترة العمل
- عند انتهاء فترة العمل أو إنهائها

٤-١ يجب على منسوبي الجامعة فهم أدوارهم الوظيفية، والشروط والمسؤوليات ذات العلاقة بالأمن السيبراني، والموافقة عليها.

٥-١ يجب تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Agreement) في عقود منسوبي الجامعة (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع جامعة الملك فيصل).

٦-١ يجب إدراج المخالفات ذات العلاقة بالأمن السيبراني في لائحة مخالفات الموارد البشرية في جامعة الملك فيصل.

٧-١ يُمنع الاطلاع على المعلومات الخاصة بالموظفين دون تصريح مسبق.

٨-١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالموارد البشرية.

قبل التوظيف

٢-١ يجب على العاملين التعهد بالالتزام بسياسات الأمن السيبراني قبل منحهم صلاحية الوصول إلى أنظمة الجامعة.

٢-٢ يجب تحديد أدوار الموظفين ومسؤولياتهم مع الأخذ في الحسبان تطبيق مبدأ عدم تعارض المصالح.

٢-٣ يجب تحديد أدوار الموظفين ومسؤولياتهم المتعلقة بالأمن السيبراني في الوصف الوظيفي.

٢-٤ يجب أن تشمل الأدوار والمسؤوليات المتعلقة بالأمن السيبراني الآتي:

- حماية جميع أصول الجامعة من الوصول غير المصرح به، أو تخريب تلك الأصول.
- تنفيذ جميع الأنشطة المطلوبة المتعلقة بالأمن السيبراني.
- الالتزام بسياسات الأمن السيبراني ومعاييره الخاصة بالجامعة.

٢-٥ يجب إجراء مسح أمني للعاملين في وظائف الأمن السيبراني، والوظائف التقنية ذات الصلاحيات الهامة والحساسة، والوظائف ذات العلاقة بالأنظمة الحساسة.

أثناء العمل

٣-١ يجب تقديم برنامج توعوي يختص بزيادة مستوى الوعي بالأمن السيبراني لدى منسوبي الجامعة، بما في ذلك سياسات الأمن السيبراني ومعاييره وذلك بشكل دوري.

٣-٢ يجب على الجهة/الجهات المسؤولة عن الموارد البشرية بالجامعة إبلاغ عمادة تقنية المعلومات والإدارات ذات العلاقة عن أي تغيير في أدوار العاملين أو مسؤولياتهم، وذلك بهدف اتخاذ الإجراءات اللازمة المتعلقة بإلغاء صلاحيات الوصول أو تعديلها.

٣-٣ يجب التأكد من تطبيق متطلبات الأمن السيبراني الخاصة بالموارد البشرية.

٣-٤ يجب التأكد من تطبيق مبدأ الحاجة إلى المعرفة (Need-to-know) في تكليف المهمات.

انتهاء الخدمة أو إنهاؤها

٤-١ يجب تحديد إجراءات انتهاء الخدمة المهنية أو إنهائها بشكل يغطي متطلبات الأمن السيبراني.

٤-٢ يجب على الجهة/الجهات المسؤولة عن الموارد البشرية بالجامعة إبلاغ الوحدات ذات العلاقة في حال اقتراب موعد انتهاء العلاقة الوظيفية أو إنهائها لاتخاذ الإجراءات اللازمة.

٤-٣ يجب التأكد من إعادة جميع الأصول الخاصة بالجامعة وإلغاء صلاحيات الدخول للعاملين في آخر يوم عمل لهم وقبل حصولهم على المخالصات اللازمة.

٤-٤ يجب تحديد المسؤوليات والواجبات التي ستبقى سارية المفعول بعد انتهاء خدمة منسوبي الجامعة، بما في ذلك اتفاقية المحافظة على سرية المعلومات، على أن يتم إدراج تلك المسؤوليات والواجبات في جميع عقود العاملين.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** الجهة/الجهات المسؤولة عن الموارد البشرية بالجامعة.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١١. سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية، وحماية الأصول المعلوماتية لجامعة الملك فيصل من التهديدات (Threats) الداخلية والخارجية، عن طريق استخدام نظام إدارة سجلات الأحداث، ومراقبة الأمن السيبراني.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة إدارة سجلات الأحداث، ومراقبة الأمن السيبراني الخاصة بجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- البنود العامة

١-١ يجب توفير تقنيات إدارة المعلومات، والأحداث الأمنية (*Security Information and Event Management "SIEM"*) اللازمة، وذلك لجمع سجلات الأحداث السيبرانية للأصول المعلوماتية والأنظمة والتطبيقات وقواعد البيانات والشبكات وأنظمة الحماية في الجامعة. ويجب أن تحتوي هذه السجلات على المعلومات الآتية بوصفها حداً أدنى:

١-١-١ نوع الحدث (Event Type)

١-١-٢ مكان الحدث، أو النظام الذي تم تنفيذ الحدث عليه (Location of Event or System)

١-١-٣ وقت الحدث وتاريخه (Date and Time of Event)

١-١-٤ المستخدم أو الأداة المستخدمة لتنفيذ الحدث

١-١-٥ حالة الحدث أو نتيجته (Success vs. Failure)

٢- الأحداث المراد تسجيلها

٢-١ يجب أن تفعّل الأنظمة المراد مراقبتها سجلات الأحداث عند وقوع أحد الأحداث، بحد أدنى ما يلي:

٢-١-١ الأحداث (Event Logs) الخاصة بالأمن السيبراني على جميع المكونات التقنية للأنظمة الحساسة (أنظمة التشغيل، قواعد البيانات، التخزين، التطبيقات، والشبكات).

٢-١-٢ الأحداث (Event Logs) الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها.

٢-١-٣ الأحداث الخاصة بالحسابات التي تمتلك صلاحيات مهمة وحساسة على الأصول المعلوماتية.

٢-١-٤ الأحداث الخاصة بالتصفح والاتصال بالإنترنت، والشبكة اللاسلكية.

٢-١-٥ نقل المعلومات عبر وسائط التخزين الخارجية.

٢-١-٦ إجراء تغييرات غير مشروعة على السجلات، وملفات الأنظمة الحساسة من خلال تقنيات إدارة تغييرات الملفات (File Integrity Management "FIM").

٢-١-٧ تغيير إعدادات النظام أو الشبكة أو الخدمات بما في ذلك تنزيل حزم التحديثات والإصلاحات أو غيرها من التغييرات على البرامج المثبتة.

٢-١-٨ أنشطة مشبوهة، مثل الأنشطة التي يكتشفها نظام منع التسلل (Intrusion Prevention System "IPS")

٢-٢ يجب إعداد إجراءات ومعايير أمنية تطبق أفضل الممارسات لحفظ سجلات الأحداث بطريقة تضمن سلامتها من التعديل، أو الحذف، أو الوصول غير المصرح به.

٢-٣ يجب مراقبة سجلات الأحداث، وتحليلها دورياً حسب تصنيفها، بما في ذلك مراقبة سلوك مستخدم الأنظمة الحساسة وتحليله.

٢-٤ يجب مزامنة التوقيت (Clock Synchronization) مركزياً، ومن مصدر دقيق وموثوق، لجميع الأنظمة التي تتم مراقبتها.

٢-٥ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

٢-٦ يجب أرشفة سجلات الأحداث، والقيام بالنسخ الاحتياطي دورياً.

٢-٧ يجب أن تكون مدة الاحتفاظ بسجلات الأحداث السيبرانية ١٢ شهراً على الأقل، و١٨ شهراً بالنسبة للأنظمة الحساسة بحد أدنى، وبما يتوافق مع السياسات الداخلية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٢. سياسة إدارة حزم التحديثات والإصلاحات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ٢-٣-٣-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات وأجهزة وأنظمة التحكم الصناعي الخاصة بجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- يجب إدارة حزم التحديثات والإصلاحات (Patch Management) بشكل يضمن حماية الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات.

٢- يجب تنزيل حزم التحديثات والإصلاحات من مصادر مرخصة وموثوقة وفقاً للإجراءات المتبعة داخل الجامعة.

٣- يجب استخدام أنظمة تقنية موثوقة وآمنة لإجراء مسح دوري للكشف عن الثغرات وحزم التحديثات ومتابعة تطبيقها.

٤- يجب على الأقسام ذات العلاقة بعمادة تقنية المعلومات اختبار حزم التحديثات والإصلاحات في البيئة الاختبارية (Test Environment) قبل تثبيتها على الأنظمة والتطبيقات وأجهزة معالجة المعلومات في بيئة الإنتاج (Production Environment)، للتأكد من توافق حزم التحديثات والإصلاحات مع الأنظمة والتطبيقات.

٥- يجب وضع خطة للاسترجاع (Rollback Plan) وتطبيقها في حال تأثير حزم التحديثات والإصلاحات سلباً على أداء الأنظمة أو التطبيقات أو الخدمات.

٦- يجب على اللجنة الإشرافية للأمن السيبراني في الجامعة التأكد من تطبيق حزم التحديثات والإصلاحات دورياً.

٧- يجب منح الأولوية لحزم التحديثات والإصلاحات التي تعالج الثغرات الأمنية حسب مستوى المخاطر المرتبطة بها.

٨- يجب جدولة التحديثات والإصلاحات بما يتماشى مع مراحل الإصدارات البرمجية التي يطرحها المورد.

٩- يجب تنصيب التحديثات والإصلاحات مرّة واحدة شهرياً على الأقل للأنظمة الحسّاسة المتصلة بالإنترنت، ومرّة واحدة كل ثلاثة أشهر للأنظمة الحسّاسة الداخلية. (CSCC-2-3-1-3).

١٠- يجب تنصيب التحديثات والإصلاحات للأصول التقنية على النحو الموضح بالجدول التالي (جدول رقم: ٩ - مدة تكرار تنصيب التحديثات والإصلاحات):

نوع الأصل	مدة التكرار لتنصيب التحديثات	
	الأصول المعلوماتية والتقنية	الأصول المعلوماتية والتقنية للأنظمة الحساسة
أنظمة التشغيل	شهرياً	شهرياً
قواعد البيانات	ثلاثة أشهر	شهرياً
أجهزة الشبكة	ثلاثة أشهر	شهرياً
التطبيقات	ثلاثة أشهر	شهرياً

١١- يجب أن تتبع عملية إدارة التحديثات والإصلاحات متطلّبات عملية إدارة التغيير.

١٢- في حال وجود ثغرات أمنية ذات مخاطر عالية، يجب تنصيب حزم التحديثات والإصلاحات الطارئة وفقاً لعملية إدارة التغيير الطارئة (Emergency Change Management).

١٣- يجب تنزيل التحديثات والإصلاحات على خادم مركزي (Server Centralized Patch Management) قبل تنصيبها على الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات، ويُستثنى من ذلك حزم التحديثات والإصلاحات التي لا يتوفر لها أدوات آلية مدعومة.

١٤- بعد تنصيب حزم التحديثات والإصلاحات، يجب استخدام أدوات مستقلة وموثوقة للتأكد من أن الثغرات تمت معالجتها بشكل فعال.

١٥- يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لإدارة حزم التحديثات والإصلاحات.

١٦- يجب مراجعة سياسة إدارة حزم التحديثات والإصلاحات وإجراءاتها سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.

- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٣. سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني لضمان حماية الأصول المعلوماتية والتقنية في جامعة الملك فيصل من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإسناد لتقنية المعلومات والخدمات المدارة وفقا للسياسات والإجراءات التنظيمية الخاصة بجامعة الملك فيصل.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-١-٤ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تنطبق هذه السياسة على جميع الخدمات المقدمة من الأطراف الخارجية لجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- **البنود العامة**

١-١ يجب توثيق واعتماد إجراءات موحدة لإدارة علاقة جامعة الملك فيصل مع الأطراف الخارجية قبل وأثناء وبعد انتهاء العلاقة التعاقدية.

١-٢ يجب تحديد واختيار الأطراف الخارجية المقدمة للخدمات بعناية ووفقاً للسياسات والإجراءات التنظيمية لجامعة الملك فيصل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب إجراء تقييم للمخاطر على الأطراف الخارجية والخدمات المقدمة والتأكد من سلامتها، وذلك بمراجعة مشاريع الأطراف الخارجية داخل الجامعة ومراجعة سجلات الأحداث السيبرانية الخاص بخدمة الطرف الخارجي (إن أمكن) قبل وأثناء العلاقة وبشكل دوري.

١-٤ يجب إعداد العقود والاتفاقيات مع الأطراف الخارجية بشكل يضمن التزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجامعة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٥ يجب مراجعة العقود والاتفاقيات مع الأطراف الخارجية من قبل الجهة المعنية بالشؤون القانونية في الجامعة للتأكد من أن تكون بنود الاتفاقية ملزمة أثناء فترة العقد وبعد انتهائها وأن مخالفتها يعرض الطرف الخارجي للمساءلة قانونياً.

١-٦ يجب أن تشمل العقود والاتفاقيات على بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الأمن من قِبَل الطرف الخارجي لبيانات الجامعة عند انتهاء الخدمة.

١-٧ يجب مراجعة متطلبات الأمن السيبراني مع الأطراف الخارجية بشكل دوري.

١-٨ يجب مراجعة سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية سنوياً، وتوثيق التغييرات واعتمادها.

٢- متطلبات الأمن السيبراني الخاصة بخدمات الإسناد لتقنية المعلومات "Outsourcing" أو الخدمات المدارة "Managed Services" المقدمة من قبل الأطراف الخارجية

١-٢ للحصول على خدمات إسناد لتقنية المعلومات أو خدمات مدارة، فإنه يجب اختيار الطرف الخارجي بعناية، ويجب أن يتم التحقق من الآتي:

١-١-٢ إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١-٢ يجب أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة والتي تستخدم طريقة الوصول عن بعد موجودة بالكامل داخل المملكة. (ECC-4-1-3-2)

٣-١-٢ خدمات الإسناد على الأنظمة الحساسة يجب أن تكون عن طريق شركات وجهات وطنية، وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. (CSCC-4-1-1-2)

٣- متطلبات الأمن السيبراني المتعلقة بموظفي الأطراف الخارجية

١-٣ يجب أن يتم إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة العاملين على الأنظمة الحساسة. (CSCC-4-1-1-1)

٢-٣ يجب تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) في عقود موظفي الأطراف الخارجية (لتشمل خلال وبعد انتهاء/ إنهاء العلاقة الوظيفية مع الجامعة).

٤- التوثيق وضوابط الوصول

١-٤ يجب أن تُطوّر الأطراف الخارجية وتتبع عملية رسمية وموثّقة بعناية لمنح وإلغاء حق الوصول إلى جميع الأنظمة المعلوماتية والتقنية التي تُعالِج أو تنقل أو تخزّن معلومات الجامعة بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بالجامعة.

٢-٤ يجب توفير إمكانية الوصول إلى معلومات الجامعة ومعالجتها بطريقة آمنة ومراقبة.

٣-٤ يجب تطبيق الضوابط المتعلّقة بكلمات المرور على جميع المستخدمين الذين يملكون حق الوصول إلى معلومات الجامعة بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بالجامعة.

٤-٤ يجب تطبيق نظام التحقّق من الهوية متعدّد العناصر على إمكانية الوصول إلى الأنظمة الحسّاسة التي تُعالج المعلومات الخاصة بالجامعة أو تنقلها أو تُخزّنها.

٥-٤ يجب إلغاء حقوق الوصول فور انتهاء/إنهاء خدمات أي موظف يعمل لدى الأطراف الخارجية ويملك حق الوصول إلى المعلومات أو الأصول المعلوماتية والتقنية الخاصة بالجامعة أو في حال تغيير دوره الوظيفي الذي لا يتطلّب استمرارية وصوله إليها.

٦-٤ يجب أن تقوم الأطراف الخارجية بمراجعة حقوق الوصول بوتيرة دورية وفقًا لسياسات الأمن السيبراني المعتمدة في الجامعة.

٧-٤ يجب تخزين كلّ سجلات التدقيق والحفاظ عليها وتوفيرها بناءً على طلب الجامعة.

٥- متطلبات الأمن السيبراني المتعلقة بإدارة التغيير

١-٥ يجب أن تتبع الأطراف الخارجية عملية إدارة التغيير الرسمية والمناسبة وفقاً لسياسات وإجراءات الجامعة وبما يتوافق مع متطلّبات الأمن السيبراني.

٢-٥ يجب مراجعة واختبار التغيير التي أجريت على الأصول المعلوماتية والتقنية الخاصة بالجامعة قبل تطبيقها على بيئة الإنتاج (Production Environment).

٣-٥ يجب إبلاغ الأطراف المعنية في الجامعة بالتغييرات الرئيسية التي مخطط إجراءها وكذلك التي أجريت على الأصول المعلوماتية والتقنية الخاصة بالجامعة.

٦- متطلبات إدارة حوادث الأمن السيبراني واستمرارية الأعمال

١-٦ يجب ان تتضمن بنود العقود والاتفاقيات مع الأطراف الخارجية على متطلبات متعلقة بالإبلاغ عن حوادث الأمن السيبراني وإبلاغ الجامعة في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني.

٢-٦ يجب تحديد وتوثيق إجراءات التواصل بين الطرف الخارجي والجامعة في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني، ومراجعة وتحديث هذه الإجراءات بشكل دوري.

٣-٦ يجب وضع خطة مناسبة لاستمرارية الأعمال لتفادي عدم توافر الخدمات المقدمة للجامعة وفقاً لمتطلّبات خطّة استمرارية الأعمال الخاصة بالجامعة.

٧- متطلبات حماية البيانات والمعلومات

١-٧ يجب أن تقوم الأطراف الخارجية بمعالجة بيانات ومعلومات الجامعة وتخزينها وإتلافها وفقاً لسياسة ومعيار حماية البيانات والمعلومات المعتمدين في الجامعة.

٢-٧ يجب تطبيق ضوابط تشفير مناسبة لحماية بيانات ومعلومات الجامعة وضمان الحفاظ على سريّتها وسلامتها وتوافرها وفقاً لمعيار التشفير المعتمد في الجامعة.

٣-٧ يجب عمل نُسخ احتياطية من بيانات ومعلومات الجامعة بشكل دوري ووفقاً لسياسة إدارة النسخ الاحتياطية الخاصة بالجامعة.

٤-٧ يجب عدم معالجة أو تخزين أو استخدام بيانات ومعلومات الجامعة الموجودة في الأنظمة الحسّاسة والبيانات الشخصية (Data privacy)، والتي تُعالجها الأطراف الخارجية - في بيئة الاختبار إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل: تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling) أو تقنيات إخفاء البيانات Data (Anonymization). (CSCC-2-6-1-1)

٧-٥ يجب عدم نقل بيانات ومعلومات الجامعة الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - خارج بيئة الإنتاج. (CSCC-2-6-1-5)

٧-٦ يجب تصنيف بيانات ومعلومات الجامعة الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - وفقاً لسياسة حماية وتصنيف البيانات والمعلومات (CSCC-2-6-1-2).

٨- التدقيق

٨-١ يجب أن تُجري الجامعة تدقيقاً للعمليات والأنظمة ذات الصلة متى كان ذلك ضرورياً أو مناسباً.

٨-٢ يجب أن تتعاون جميع مرافق الطرف الخارجي وموظفيه بصورة كاملة مع أنشطة مراجعة سجل الأحداث والتدقيق التي تقوم بها الجامعة بما يشمل المراجعات المُنفّذة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **تحديث السياسة ومراجعتها:** إدارة الأمن السيبراني.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني والأقسام ذات العلاقة بعمادة تقنية المعلومات والجهة/الجهات المسؤولة عن الموارد البشرية بالجامعة والجهة المعنية بالشؤون القانونية في الجامعة والجهات المعنية بعمليات المشتريات والمناقصات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٤. سياسة اختبار الاختراق

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير في تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في جامعة الملك فيصل وذلك من خلال محاكاة تقنيات وأساليب الهجوم السيبراني الفعلية، ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني للجامعة من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة الحساسة ومكوناتها التقنية، وجميع الخدمات المقدمة خارجياً (عن طريق الإنترنت)ومكوناتها التقنية، ومنها: البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، تطبيقات الهواتف الذكية واللوحية،والبريد الإلكتروني والدخول عن بعد في جامعة الملك فيصل، وتنطبق هذه السياسة على جميع منسوبي الجامعة.

بنود السياسة

١- المتطلبات العامة

١-١ يجب على الجامعة إجراء اختبار الاختراق (Penetration Testing) دورياً، لتقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني.

١-٢ تحدد إدارة الأمن السيبراني الأنظمة والخدمات والمكونات التقنية التي يجب إجراء اختبار الاختراق عليها وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب على الجامعة إجراء اختبار الاختراق على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية دورياً. (ECC-2-11-3-1)

١-٤ يجب التأكد من أن اختبار الاختراق لا يؤثر على الأنظمة والخدمات المقدمة في الجامعة.

١-٥ يجب على الجامعة إجراء اختبار الاختراق على الأنظمة الحساسة ومكوناتها التقنية كل ١٢ شهر على الأقل. (CSCC-2-10-2)

١-٦ يجب إجراء اختبار الاختراق لاكتشاف نقاط الضعف الأمنية بكافة صورها والتي تشمل نقاط الضعف التي تنتج عادةً عن أخطاء في تطوير التطبيقات (Application Development Error) وضبط إعدادات النظام بشكل غير آمن (Configurations Faults) وإمكانية استغلال ثغرة محددة (Exploitability of Identified Vulnerability).

١-٧ يجب تطوير إجراءات خاصة باختبار الاختراق واعتمادها ونشرها، مع الأخذ بالاعتبار عدم تأثيرها على سير الأعمال الخاصة بالجامعة.

١-٨ يجب على إدارة الأمن السيبراني تحديد أو الموافقة على أساليب اختبار الاختراق والأدوات والتقنيات التي يستخدمها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.

١-٩ في حال تفويض طرف خارجي للقيام باختبار الاختراق نيابة عن الجامعة، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية ووفقاً لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة في الجامعة.

١-١٠ يجب تصنيف نتائج اختبار الاختراق بناءً على خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها ووفقاً لمنهجية إدارة المخاطر المعتمدة لدى الجامعة.

١-١١ يجب وضع خطة عمل لمعالجة نتائج اختبار الاختراق يوضح فيها تأثير المخاطر وآلية معالجتها والمسؤول عن تطبيقها والفترة الزمنية اللازمة لتنفيذها.

٢- متطلبات أخرى

٢-١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لعمليات اختبار الاختراق.

٢-٢ يجب مراجعة تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجامعة دورياً. (ECC-2-11-4)

٢-٣ يجب مراجعة هذه السياسة مرة واحدة في السنة على الأقل.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني والأقسام ذات العلاقة بعمادة تقنية المعلومات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٥. سياسة إدارة الثغرات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وكذلك التقليل من الآثار المترتبة على أعمال جامعة الملك فيصل وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٠-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية في جامعة الملك فيصل، وتنطبق هذه السياسة على جميع منسوبي الجامعة.

بنود السياسة

١- المتطلبات العامة

١-١ يجب على الجامعة إجراء فحص الثغرات (Vulnerabilities Assessment) دورياً، لاكتشاف وتقييم الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال.

١-٢ تحدد إدارة الأمن السيبراني الأنظمة والخدمات والمكونات التقنية التي يجب إجراء فحص الثغرات عليها وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب على إدارة الأمن السيبراني التأكد من استخدام أساليب وأدوات موثوقة لاكتشاف الثغرات.

١-٤ يجب تطوير واعتماد إجراءات خاصة بتنفيذ فحص واكتشاف الثغرات وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٥ في حال تفويض طرف خارجي للقيام بفحص واكتشاف الثغرات نيابة عن الجامعة، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية وفقاً لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة في الجامعة.

٢- متطلبات تقييم الثغرات

٢-١ يجب فحص واكتشاف الثغرات قبل نشر الخدمات أو الأنظمة على الإنترنت أو عند القيام بأي تغيير على الأنظمة الحساسة.

٢-٢ يجب تصنيف الثغرات حسب خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها وفقاً لمنهجية إدارة المخاطر المعتمدة لدى الجامعة.

٢-٣ يجب على الجامعة إجراء تقييم الثغرات لجميع الأصول التقنية ومعالجتها دورياً. (ECC-2-10-3-1)

٢-٤ يجب على الجامعة إجراء تقييم الثغرات للمكونات التقنية للأنظمة الحساسة الداخلية ومعالجتها كل ثلاثة أشهر على الأقل. (CSCC-2-9-1-3)

٢-٥ يجب على الجامعة إجراء تقييم الثغرات للمكونات التقنية للأنظمة الحساسة الخارجية والمتصلة بالإنترنت مرة واحدة شهرياً. (CSCC-2-9-1-2)

٣- متطلبات معالجة الثغرات

٣-١ بعد الانتهاء من تقييم الثغرات، يجب إعداد تقرير يوضح الثغرات المكتشفة وتصنيفها والتوصيات المقترحة لمعالجتها.

٣-٢ بعد إرسال تقرير تقييم الثغرات ومعالجتها من قبل الأطراف المعنية، يجب إجراء فحص واكتشاف الثغرات المكتشفة مرة أخرى للتأكد من معالجتها.

٣-٣ يجب استخدام حزم التحديثات والإصلاحات من مصادر موثوقة وآمنة ووفقاً لسياسة حزم التحديثات والإصلاحات.

٣-٤ يجب إصلاح وإغلاق الثغرات الحرجة (Critical Vulnerabilities) المكتشفة حديثاً، مع اتباع آليات إدارة التغيير المتبعة لدى الجامعة. (CSCC-2-9-1-3)

٣-٥ في حال تعذر إصلاح وإغلاق الثغرة الأمنية لأي سببٍ كان، يجب تطبيق ضوابط أخرى مثل إيقاف تشغيل الخدمة المتعلقة بالثغرة الأمنية، أو توفير ضابط حماية بديل (Compensating Control) مثل التحكم بالوصول عن طريق جدران الحماية وغيرها من الحلول، ومراقبة الثغرة الأمنية للهجمات الفعلية، وإبلاغ فريق الاستجابة للحوادث بهذه الثغرة واحتمالية استغلالها.

٤- متطلبات أخرى

٤-١ يجب على الجامعة التواصل والاشتراك مع مصادر أمن سيبراني موثوقة توفر المعلومات الاستباقية (Threat Intelligence)، ومجموعات خاصة ذات اهتمامات مشتركة وخبراء خارجيين في المواضيع المعنية من أجل جمع المعلومات حول التهديدات الجديدة وكيفية الحد من الثغرات الموجودة. (ECC-2-10-3-5)

٤-٢ يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية لجامعة الملك فيصل دورياً.

٤-٣ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الثغرات.

٤-٤ يجب مراجعة هذه السياسة مرة واحدة في السنة على الأقل.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني والأقسام ذات العلاقة بعمادة تقنية المعلومات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٦. سياسة إدارة حوادث وتهديدات الأمن السيبراني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حوادث وتهديدات الأمن السيبراني الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل، وتنطبق هذه السياسة على جميع منسوبي الجامعة.

بنود السياسة

١- المتطلبات العامة

١-١ يجب على الجامعة توفير التقنيات اللازمة لتحديد حوادث الأمن السيبراني واكتشافها في الوقت المناسب أو من خلال استلام البلاغات من العاملين أو المستفيدين من خدمات الجامعة وإدارتها بشكل فعال.

١-٢ يجب على الجامعة التعامل مع تهديدات الأمن السيبراني استباقياً باعتماد وسائل دفاع وقائية من أجل منع أو تقليل الآثار المترتبة على سرية المعلومات أو سلامتها أو توافرها.

١-٣ تشمل حوادث الأمن السيبراني على سبيل المثال لا الحصر ما يلي:

١-٣-١ التغييرات غير المصرح بها في إعدادات أجهزة المستخدمين المكتبية و/أو المحمولة، والتغييرات في إعدادات الخوادم.

١-٣-٢ الإصابة بالبرمجيات الضارة.

١-٣-٣ التغييرات في التطبيقات من حيث المظهر (المظهر غير الاعتيادي) والتعديلات على صلاحيات المستخدم مثل رفع مستوى الوصول.

١-٣-٤ الوصول غير المصرح به إلى البيانات، و/أو تعديلها دون تصاريح أو صلاحيات المستخدمين.

١-٣-٥ محاولات الحصول على معلومات يمكن استخدامها في تنفيذ الهجمات، مثل فحص منافذ الشبكة (Port Scans)، والهندسة الاجتماعية (Social Engineering Attacks)، وفحص مجال شبكة محددة (Targeted Scans Across IP Range)، وغيرها.

١-٣-٦ التفعيل غير المصرح به لحسابات مستخدمين موقوفة أو محذوفة.

١-٤ يجب توثيق الأدوار والمسؤوليات الخاصة بفريق الاستجابة للحوادث السيبرانية وكذلك وضع خطط الاستجابة للحوادث الأمنية وآليات التصعيد وصلاحيات اتخاذ القرارات الهامة. (ECC-2-13-3-1)

١-٥ في حال اكتشاف حادثة أمن سيبراني في الجامعة، يجب على فريق الاستجابة للحوادث اتخاذ الخطوات اللازمة للتعامل مع الحادثة التي تم اكتشافها فوراً والتي تشمل تحليل بيانات الحادثة وتحديد أثرها.

١-٦ في حال اكتشاف حادثة أمن سيبراني فإنه يجب تحليل المعلومات المتاحة ذات العلاقة مثل سجلات النظام والشبكة والسجلات الصادرة من المنتجات الأمنية ذات الصلة (مثل السجلات الصادرة من حلول الحماية من البرمجيات الضارة، ومن جدار الحماية، ومن أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات).

١-٧ يجب معالجة الأدلة اللازمة (على سبيل المثال، جمع الأدلة وفقاً للقيود القانونية وحمايتها من التلاعب) وينبغي توثيقها وحفظها بصورة محمية حتى لا تفقد جدواها في التحليل، ثم تحليلها دون تدميرها أو تعديل صورتها الأصلية.

١-٨ في حال وقوع حادثة أمن سيبراني فإنه يجب التحقيق في أسباب حدوثها والاستعانة بالمختصين مثل خبراء التحليل الجنائي الرقمي (Digital Forensics Analysts) وفرق الاستجابة للحوادث السيبرانية.

١-٩ يجب تصنيف حوادث الأمن السيبراني بناءً على مستوى خطورتها ومدى تأثيرها على أعمال الجامعة (ECC-2-13-3-2).

١-١٠ يتم تصنيف حوادث الأمن السيبراني وفقاً للجدول أدناه (جدول رقم: ١٠ - تصنيف حوادث الأمن السيبراني):

مستوى الخطورة	الوصف	الوقت المستهدف للاستجابة	الوقت المستهدف لحل الحادثة
مرتفع جداً	ضرر جسيم يؤثر بشكل مباشر على سمعة جامعة الملك فيصل ومصداقيتها، أو يؤثر على العديد من وحدات الأعمال الوظيفية فيها أو موقع الأعمال بصورة كبيرة، مما يستدعي تفعيل إجراءات استمرارية الأعمال.	فوراً	ساعتان
مرتفع	انقطاع كبير يؤثر على وحدات الأعمال الوظيفية أو الخدمات الرئيسية أو الموقع.	ساعة أو ساعتان	٤-٥ ساعات
متوسط	تأثير متوسط في سير عمل وحدات الأعمال الوظيفية أو المواقع أو أصول تقنية المعلومات، إضافة إلى تأثير يتراوح ما بين المتوسط والمرتفع على وحدات الأعمال غير الهامة في جامعة الملك فيصل.	٢-٣ ساعات	٨-٩ ساعات
منخفض	تأثير بسيط على عدد قليل من الموارد، ويمكن تحمل الحادثة لفترة معينة من الزمن.	٥ ساعات	٢٤ ساعة

٢- الإبلاغ عن حوادث الأمن السيبراني

٢-١ يجب رفع الوعي الأمني لدى منسوبي الجامعة وتوضيح مسؤولياتهم تجاه حوادث الأمن السيبراني أو التهديدات، وذلك للإبلاغ فوراً عن أي حوادث أو تهديدات متعلقة بالأمن السيبراني.

٢-٢ يجب على الجامعة تحديد جهة اتصال داخلية للإبلاغ عن الحوادث سواءً عن طريق الهاتف أو البريد الإلكتروني.

٢-٣ يجب أن تحدد الجامعة الحوادث والتهديدات التي يجب الإبلاغ عنها ووقت الإبلاغ عنها والأطراف التي يجب إبلاغها، مثل معالي رئيس الجامعة أو من ينيبه والمسؤول على إدارة الأمن السيبراني وفرق الاستجابة للحوادث داخل الجامعة والإدارات المسؤولة عن الأصول المعلوماتية والتقنية.

٢-٤ قبل الإفصاح عن أي معلومات متعلقة بالحوادث الأمنية إلى أطراف خارجية، يجب الحصول على الموافقات اللازمة بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٥ يجب إبلاغ الهيئة الوطنية للأمن السيبراني عن حوادث الأمن السيبراني. (ECC-2-13-3-3)

٢-٦ يجب على الجامعة إطلاع الهيئة الوطنية للأمن السيبراني على تبليغات الحوادث ومؤشرات وتقارير الانتهاكات (ECC-2-13-3-4).

٣- الاستجابة للحوادث والتعافي من حوادث الأمن السيبراني

٣-١ يجب على فريق الاستجابة للحوادث في إدارة الأمن السيبراني كتابة تقرير عن حوادث الأمن السيبراني، ويجب أن يشمل التقرير نوع الحادثة وفئتها والعاملين الذين أبلغوا عن الحادثة أو الأدوات المستخدمة في اكتشافها، والخدمات أو الأصول أو المعلومات المتأثرة بها، وكيفية اكتشاف الحادثة، وأي وثائق أو موارد أخرى متعلقة بالحادثة.

٣-٢ يجب أن يتم إشراك الموردين في حل الحوادث أو استعادة الخدمات عند الحاجة.

٣-٣ يجب أن تتضمن إجراءات التعافي من حوادث الأمن السيبراني تحديد الثغرات التي تم استغلالها خلال الحادثة ومعالجتها بالتدابير الفنية والإدارية اللازمة، على سبيل المثال:

٣-٣-١ تطبيق الضوابط الأمنية الإضافية (Compensating Controls).

٣-٣-٢ تنصيب حزم التحديثات والإصلاحات المحدثة.

٣-٣-٣ استعادة النسخ الاحتياطية للنظام.

٣-٣-٤ إعادة ضبط إعدادات الأنظمة الأمنية، مثل نظام جدار الحماية وأنظمة الكشف عن الاختراق.

٣-٤ يجب على إدارة الأمن السيبراني حفظ تقارير الحادثة (التي تتضمن معلومات حول الاختراقات الأمنية والحوادث مثل المعلومات المتعلقة بالأفراد والإدارات وأنظمة معينة و/أو منهجية الهجمات) بمكان آمن وتقييد الوصول إليها.

٣-٥ يجب تصعيد الحادثة، في حال عدم حلها في الوقت الزمني المحدد، وفقاً لتصنيف الحوادث وإجراءات التعامل معها وآلية التصعيد المعتمدة.

٣-٦ في حال تطلبت معالجة حادثة سيبرانية إجراء تغييرات على المكونات التقنية، يجب الالتزام بإجراءات إدارة التغيير المعتمدة لدى الجامعة.

٣-٧ بعد التعامل مع الحادثة فإنه يجب على فريق الاستجابة للحوادث في إدارة الأمن السيبراني عقد اجتماعات لمناقشة الدروس المستفادة (Lessons Learned) مع الإدارات ذات العلاقة لتحسين طرق التعامل مع حوادث الأمن السيبراني في

المستقبل، وكذلك التعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال جامعة الملك فيصل.

٤- **المعلومات الاستباقية بشأن التهديدات**

٤-١ يجب الاشتراك مع مقدمي المعلومات الاستباقية (Threat Intelligence) للاطلاع المستمر على الحوادث والتهديدات المتعلقة بالأمن السيبراني والتعامل مع تلك المعلومات بشكل مباشر. (ECC-2-13-3-5)

٤-٢ يجب حفظ المعلومات الاستباقية بشأن التهديدات وتنظيمها في قاعدة بيانات مرنة وملائمة لصياغة ملاحظات العمل والبيانات الوصفية للمؤشرات، مثل قاعدة المعرفة (Knowledge Base).

٤-٣ يجب تحديث أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (and Detection Systems Intrusion Prevention) بالمعلومات الاستباقية المتعلقة بالتهديدات والتأكد من إمكانية تلك الأنظمة من اكتشاف التهديدات والتعامل معها بشكل فعال.

٥- **متطلبات أخرى**

٥-١ يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة حوادث وتهديدات الأمن السيبراني دورياً. (ECC-2-13-4)

٥-٢ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة حوادث وتهديدات الأمن السيبراني.

٥-٣ يجب مراجعة هذه السياسة مرة واحدة في السنة على الأقل.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني والأقسام ذات العلاقة بعمادة تقنية المعلومات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٧. سياسة أمن قواعد البيانات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية قواعد البيانات (Database) الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط ١-٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة قواعد البيانات الخاصة بجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- **البنود العامة**

١-١ يجب تحديد وتوثيق جميع أنظمة قواعد البيانات المستخدمة داخل الجامعة والعمل على توفير البيئة المناسبة لحمايتها من المخاطر البيئية والتشغيلية.

١-٢ يجب تطوير واعتماد معايير التقنية الأمنية لأنظمة قواعد البيانات داخل الجامعة وتطبيقها من قبل مشرفي قواعد البيانات.

١-٣ فيما عدا مشرفي قواعد البيانات، يمنع الوصول أو التعامل المباشر مع قواعد البيانات الخاصة بالأنظمة الحساسة، ويتم ذلك من خلال التطبيقات فقط. (CSCC-2-2-1-8)

١-٤ يتم منح حق الوصول إلى قواعد البيانات وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

٢- **الإجراءات الأمنية المطلوبة لاستضافة قواعد البيانات**

٣-٤ التحديد الواضح لمتطلبات استمرارية الأعمال والتعافي من الكوارث الخاصة بقواعد البيانات المستضافة في العقود المعنية مع مزوّد الخدمة السحابية، والتي تتضمّن الأدوار والمسؤوليات المتبادلة من حيث النسخ الاحتياطية والاستجابة للحوادث وخطة التعافي من الكوارث وغيرها.

٣-٥ توفير العزل المنطقي بين قواعد البيانات الخاصة بالجامعة وقواعد البيانات المستضافة الأخرى.

٣-٦ يجب أن يكون موقع الاستضافة الخاص بالخدمات السحابية موجوداً ضمن النطاق الجغرافي للمملكة العربية السعودية. (ECC-3-3-2-4)

٣-٧ تقييد صلاحية الوصول الإداري إلى قواعد البيانات باستخدام وسيلة تشفير مُحكَمة مثل بروتوكول النقل الأمن (SSH)، أو الشبكات الخاصة الافتراضية (VPN)، أو طبقة المنافذ الآمنة (SSL)/أمن طبقة النقل (TLS)، وذلك وفقاً لسياسة التشفير المعتمدة في الجامعة.

٣- المتطلبات المتعلّقة بإدارة التغييرات على أنظمة قواعد البيانات

٣-١ يجب أن تتم التغييرات على قواعد البيانات (مثل ترحيل قواعد البيانات، والنقل إلى بيئة الإنتاج) وفقاً لعملية إدارة التغيير.

٣-٢ يتم تثبيت التحديثات والإصلاحات على نظام قواعد البيانات وفقاً لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة في الجامعة.

٣-٣ التأكد من استخدام أنظمة قواعد بيانات موثوقة ومعتمدة ومرخصة.

٣-٤ التأكد من وجود خطة واضحة للتعافي من الكوارث خاصة بأنظمة قواعد البيانات.

٣-٥ يجب على الجامعة توقيع اتفاقية مستوى الخدمة للدعم مع المورّدين فيما يتعلّق بنظام إدارة قواعد البيانات في بيئة الإنتاج.

٣-٦ تطبيق التجزئة والتشفير على قواعد البيانات المخزنة وفقاً لسياسة التصنيف وسياسة التشفير المعتمدة في الجامعة.

٤- مراقبة سجلات الأحداث المتعلقة بنظام قواعد البيانات

٤-١ تفعيل وحفظ سجلات الأحداث الخاصة بنظام قواعد البيانات وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة في الجامعة.

٤-٢ يجب على إدارة الأمن السيبراني مراقبة سجلات الأحداث المتعلقة بقواعد البيانات الخاصة بالأنظمة الحساسة، ومراقبة سلوك المستخدمين.

٤-٣ يجب على إدارة الأمن السيبراني مراقبة سجلات الأحداث الخاصة بمشرفي قواعد البيانات ومراقبة سلوكهم ومراجعتها دورياً.

٥- المتطلبات التشغيلية

٥-١ توفير المتطلبات اللازمة لتشغيل قواعد البيانات بشكل آمن وملائم، مثل توفير بيئة مناسبة وآمنة، وتقييد الوصول المادي إلى الأنظمة والسماح بذلك للعاملين المصرح لهم فقط.

٥-٢ يجب على الأقسام ذات العلاقة في عمادة تقنية المعلومات مراقبة أنظمة قواعد البيانات التشغيلية والتأكد من جودة أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحوه.

٥-٣ مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أنظمة قواعد البيانات. (ECC-2-3-3-4)

٦- متطلبات أخرى

٦-١ استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لنظام إدارة قواعد البيانات.

٦-٢ مراجعة متطلبات الأمن السيبراني الخاصة بإدارة قواعد البيانات سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**

- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** الأقسام ذات العلاقة في عمادة تقنية المعلومات وإدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٨. سياسة حماية تطبيقات الويب

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية تطبيقات الويب الخارجية الخاصة بجامعة الملك فيصل، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع تطبيقات الويب الخارجية الخاصة بجامعة الملك فيصل، وتنطبق هذه السياسة على جميع منسوبي الجامعة.

بنود السياسة

١- المتطلبات العامة

١-١ يجب أن تتبع تطبيقات الويب الخارجية التي يتم شراؤها أو تطويرها داخلياً مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). (ECC-2-15-3-2)

٢-١ يجب استخدام مبدأ المعمارية متعددة المستويات لتطبيقات الويب الخارجية للأنظمة الحساسة على ألا يقل عدد المستويات عن ٣ مستويات (3-tier Architecture). (CSCC-2-12-2)

٣-١ يجب التأكد من استخدام بروتوكولات الاتصالات الآمنة فقط، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وأمن طبقة النقل (TLS) وغيرها. (ECC-2-15-3-3)

٤-١ يجب استخدام نظام جدار الحماية لتطبيقات الويب (Web Application Firewall "WAF") لحماية تطبيقات الويب الخارجية من الهجمات الخارجية. (ECC-2-15-3-1)

٥-١ يجب تطبيق العزل المنطقي لبيئة التطوير (Development Environment) وبيئة الاختبار (Testing Environment) عن بيئة الإنتاج (Production Environment).

٦-١ يجب استخدام تقنيات حماية البيانات والمعلومات في تطبيقات الويب الخارجية ووفقاً لسياسة حماية وتصنيف البيانات والمعلومات.

٧-١ في حال شراء تطبيقات ويب من طرف خارجي، يجب التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني في الجامعة.

٨-١ يجب تطبيق الحد الأدنى على الأقل لمعايير أمن التطبيقات وحمايتها (Ten OWASP Top) لتطبيقات الويب الخارجية للأنظمة الحساسة. (CSCC-2-12-1-2)

٢- متطلبات حق الوصول (Access Right)

٢-١ يجب استخدام التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين على تطبيقات الويب الخارجية. (ECC-2-15-3-5)

٢-٢ يجب توثيق واعتماد معايير أمنية لتطوير تطبيقات الويب، وتشمل كحد أدنى إدارة الجلسات بشكل آمن (Secure Session Management) وموثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). (CSCC-2-12-1-1)

٢-٣ ينبغي أن يقتصر حق الوصول إلى منظومات الإنتاج، وأن يتم التحكم به وفقاً للمسؤوليات الوظيفية.

٢-٤ يجب نشر سياسة الاستخدام الآمن لجميع مستخدمي تطبيقات الويب الخارجية. (ECC-2-15-3-4)

٣- متطلبات تطوير أو شراء تطبيقات الويب

٣-١ يجب إجراء تقييم لمخاطر الأمن السيبراني عند التخطيط لتطوير أو شراء تطبيقات الويب وقبل إطلاقها في بيئة الإنتاج ووفقاً لسياسة إدارة مخاطر الأمن السيبراني المعتمدة في الجامعة.

٣-٢ قبل استخدام المعلومات المحمية في بيئة الاختبار، يجب الحصول على إذن مسبق من إدارة الأمن السيبراني واستخدام ضوابط مشددة لحماية تلك البيانات، مثل: تقنيات مزج البيانات (Data Scrambling) وتقنيات تعتيم البيانات (Data Masking)، وحذفها مباشرة بعد الانتهاء من استخدامها.

٣-٣ يجب حفظ شفرة المصدر (Source Code) بشكل آمن وتقييد الوصول إليها للمصرح لهم فقط.

٣-٤ يجب إجراء اختبار الاختراق لتطبيق الويب الخارجي في بيئة الاختبار وتوثيق النتائج والتأكد من معالجة جميع الثغرات قبل إطلاق التطبيق على بيئة الإنتاج.

٣-٥ يجب إجراء فحص الثغرات للمكونات التقنية لتطبيقات الويب والتأكد من معالجتها بتثبيت حزم التحديثات والإصلاحات المعتمدة لدى الجامعة.

٤- متطلبات أخرى

٤-١ يجب مراجعة متطلبات الأمن السيبراني الخاصة بحماية تطبيقات الويب الخارجية دورياً. (ECC-2-15-4)

٤-٢ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية تطبيقات الويب الخارجية.

٤-٣ تتم مراجعة هذه السياسة مرة واحدة في السنة على الأقل.

٤-٤ يجب توعية المستفيدين ومستخدمي البوابة الإلكترونية للجامعة بسياسة الخصوصية وسرية البيانات وذلك لتفهم وموافقتهم على نوع وطبيعة البيانات التي يتم جمعها وتحليلها.

٤-٥ بمجرد زيارة المستخدم للبوابة الإلكترونية الجامعة فإنه يقوم الخادم المعني بإدارة البوابة بتسجيل بروتوكول شبكة الإنترنت IP الخاص بالمستخدم وتاريخ ووقت الزيارة وعنوان والرابط الخاص بأي موقع إلكتروني يتم تصفحه.

٤-٦ حماية الخصوصية، لكي نتمكن من مساعدتك على حماية معلوماتك الشخصية فإنه يوصى بما يلي:

* الاتصال بإدارة الأمن السيبراني بشكل فوري عندما يغلب الظن أن شخصاً ما استطاع الحصول على كلمة المرور الخاصة بالمستخدم، أو رمز الاستخدام، أو الرقم السري، أو أي معلومات سرية أخرى.
* لا تفصح عن أي معلومات سرية عبر الهاتف أو شبكة الإنترنت ما لم تتأكد من هوية الشخص أو الطرف المستقبل للمعلومة.
* استخدم متصفحا آمنا عند قيامك بإنجاز المعاملات عبر الإنترنت مع إغلاق التطبيقات غير المستخدمة على الشبكة، والتأكد من أن برنامج الحماية من الفيروسات محدث باستمرار.
* في حالة وجود أية استفسارات أو آراء حول سياسة الخصوصية، يمكن التواصل مع إدارة البوابة الإلكترونية عبر البريد الإلكتروني بالموقع.
* للحفاظ على بياناتك الشخصية، يتم تأمين عملية التخزين الإلكتروني وكذلك البيانات الشخصية المرسلة باستخدام التقنيات الأمنية المناسبة.
* تحتوي البوابة الإلكترونية على روابط لمواقع أو بوابات إلكترونية قد تستخدم طرقًا لحماية المعلومات وخصوصياتها تختلف عن الطرق المستخدمة في البوابة الإلكترونية لجامعة الملك فيصل. لذا فإن إدارة الأمن السيبراني غير مسؤولة عن محتويات وطرق وسياسات الخصوصية لهذه المواقع الأخرى، وننصح بمراجعة إشعارات الخصوصية الخاصة بتلك المواقع.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** الأقسام ذات العلاقة في عمادة تقنية المعلومات وإدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٩. سياسة التشفير

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية الخاصة بجامعة الملك فيصل وللتقليل من المخاطر السيبرانية والتهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٨-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية الإلكترونية الخاصة بجامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة، بما في ذلك الجهات التي تتعامل معها والأطراف الخارجية.

بنود السياسة

١- البنود العامة

١-١ يجب على الجامعة تطوير وتوثيق واعتماد إجراءات ومعايير خاصة بالتشفير بناءً على حاجة العمل وعلى تحليل المخاطر في الجامعة وبحيث يتوافق المستوى الأمني مع المعايير الوطنية للتشفير الصادرة من قبل الهيئة الوطنية للأمن السيبراني. وتشمل هذه الإجراءات على حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً)، وطرق استخدامها وآلية إصدار المفاتيح ونشرها واستعادتها، بالإضافة إلى إدارة النسخ الاحتياطية للمفاتيح وإجراءات إتلاف مفاتيح التشفير. (ECC-2-8-3-1)

١-٢ يجب تشفير البيانات أثناء النقل والتخزين بناءً على تصنيفها وحسب السياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وفقاً لما تصدره الهيئة الوطنية للأمن السيبراني بهذا الشأن (CSCC-2-7-1-3).

١-٤ يجب تشفير جميع بيانات الأنظمة الحساسة أثناء النقل (Data-In-Transit) (CSCC-2-7-1-1).

١-٥ يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء التخزين (Data-at-Rest) على مستوى الملفات وقاعدة البيانات أو على مستوى أعمدة محددة داخل قاعدة البيانات (CSCC-2-7-1-2).

١-٦ يجب تحديد وتوثيق الأدوار والمسؤوليات المتعلقة بإدارة البنية التحتية لمفاتيح التشفير (Key Management Infrastructure "KMI")، للأدوار التالية على الأقل:

١-٦-١ مسؤول مفاتيح وأنظمة التشفير (Keying Material Manager).

١-٦-٢ مشرفو التشفير المسؤولون عن حماية مفاتيح التشفير (Key Custodians).

١-٦-٣ المسؤولون المعنيون بإصدار الشهادات ("Certification Authorities "CAs)، بحيث تكون موثوقة وآمنة.

١-٦-٤ المسؤولون المعنيون بتسجيل الشهادات ("Registration Authorities "RAs)، بحيث تكون موثوقة وآمنة.

٢- الاستخدام الأمن للتشفير

٢-١ يجب تحديد وتوثيق كافة حلول التشفير المستخدمة (بما في ذلك الخوارزميات والبرامج والوحدات (Modules) والمكتبات (Libraries) ومكونات التشفير الأخرى) وتقييمها واعتمادها من قبل إدارة الأمن السيبراني قبل تطبيقها في الجامعة.

٢-٢ يجب التأكد من تطبيق التشفير وفقاً لحلول التشفير المعتمدة لدى الجامعة.

٢-٣ يُمنع استخدام خوارزميات التشفير المطورة داخلياً وفقاً لدليل التشفير الخاص بمشروع أمان تطبيق الويب المفتوح (OWASP).

٢-٤ يجب استخدام طرق التحقق الأمن (مثل استخدام مفاتيح التشفير العامة والتواقيع الرقمية والشهادات الرقمية) للحد من المخاطر السيبرانية ووفقاً لحلول التشفير المعتمدة في الجامعة.

٢-٥ يجب استخدام التحقق من هوية المستخدم لنقل البيانات السرية للغاية إلى أطراف خارجية باستخدام شهادات التشفير الرقمية (Digital Certificates) المعتمدة، ووفقاً لسياسة حماية وتصنيف البيانات والمعلومات.

٢-٦ يجب استخدام وسيلة تحقق من الهوية متعددة العناصر ("MFA" Multi-Factor Authentication) للتحقق من صلاحية المستخدم للوصول إلى الأنظمة الحساسة وفقاً لسياسة حماية وتشفير البيانات والمعلومات المعتمدة لدى الجامعة.

٣- إدارة مفاتيح التشفير

٣-١ يجب إدارة مفاتيح التشفير بطريقة آمنة خلال عمليات دورة حياتها (Key Lifecycle Management) والتأكد من استخدامها بشكل سليم وفعّال. (ECC-2-8-3-2)

٣-٢ يجب أن يتم إصدار شهادات التشفير عن طريق جهة إصدار الشهادات الداخلية في الجامعة للخدمات المحلية أو عن طريق جهة خارجية موثوقة.

٣-٣ يجب حفظ معلومات المفاتيح الخاصة (Private Key) في مكان آمن (وخاصة إذا كانت تستخدم للتوقيع الإلكتروني)، ومنع الوصول غير المصرح به، بما في ذلك جهات إصدار الشهادات.

٣-٤ يجب توفير التقنيات اللازمة لحماية مفاتيح التشفير عند تخزينها (Tamper Resistant Safe).

٣-٥ يجب حماية المفاتيح الخاصة (Private Key) من خلال تأمينها بكلمة مرور و/أو من خلال تخزينها على وسيط آمن، ووفقاً لإجراءات التشفير المعتمدة.

٣-٦ يجب تصنيف مفاتيح التشفير الخاصة باعتبارها معلومات "سرية للغاية" وفقاً لسياسة حماية وتصنيف البيانات والمعلومات.

٣-٧ يجب تفعيل سجلات الأحداث لحلول إدارة مفاتيح التشفير ومراقبتها دورياً.

٣-٨ يجب تحديد مدة لاستخدام مفاتيح التشفير وتاريخ الإنشاء وتاريخ الانتهاء لكل مفتاح.

٣-٩ يجب تجديد مفاتيح التشفير قبل انتهاء صلاحيتها.

٣-١٠ يجب استخدام قائمة محدثة لشهادات التشفير الملغية (Certificate Revocation List) وذلك لضمان عدم استخدام شهادات التشفير منتهية الصلاحية أو التي تعرضت لانتهاك أمني في التعاملات مستقبلاً.

٣-١١ في حال تعرض مفتاح التشفير الخاص (Private Key) المُستخدم من قبل الجامعة إلى انتهاك أمني أو في حال عدم توفر المفتاح (بسبب تلف وسائط تخزين المفاتيح)، يجب إبلاغ الجهة المعنية بإصدار الشهادات على الفور لإلغائه وإعادة إصدار مفتاح التشفير الخاص (Private Key).

٣-١٢ يجب إلزام الجهة المعنية بإصدار الشهادات، في حال تعرضت مفاتيح التشفير الخاصة بها (Keys Private) إلى انتهاك أمني، بإبلاغ الجامعة وإلغاء جميع الشهادات فوراً واستبدال المفتاح الخاص بالجهة المعنية بإصدار الشهادات.

٣-١٣ في حال عدم إمكانية تبادل المفاتيح بشكل آمن وموثوق عبر شبكات الاتصالات، يجب نقل مفاتيح التشفير باستخدام قنوات بديلة آمنة ومستقلة (out-of-band channels).

٣-١٤ يجب مراجعة وتحديث متطلبات طول مفاتيح التشفير بناءً على آخر التطورات التقنية ذات العلاقة مرة في السنة على الأقل وبما يتوافق مع معايير التشفير الوطنية.

٣-١٥ مشرفو التشفير هم المسؤولون عن حماية مفاتيح التشفير (Key Custodians) وهم المصرح لهم فقط باستبدال مفاتيح التشفير عند الحاجة.

٣-١٦ يُمنع حفظ مفاتيح التشفير على الذاكرة الرئيسية أو حفظها بنفس الأنظمة المطبق عليها التشفير. وعوضاً عن ذلك، يُوصى بحفظها على أجهزة مستقلة (Peripheral Hardware Devices)، مثل أجهزة حماية مفاتيح التشفير (Hardware Security Modules "HSM")، وأنظمة تخزين المفاتيح (Key Loaders)، أو أي أجهزة أخرى مخصصة لهذا الغرض.

٤- متطلبات أخرى

٤-١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر للاستخدام السليم والفعال للتشفير.

٤-٢ يجب مراجعة كافة متطلبات الأمن السيبراني الخاصة بالتشفير دورياً. (ECC-2-8-4)

٤-٣ تتم مراجعة هذه السياسة مرة واحدة في السنة على الأقل.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** الأقسام ذات العلاقة في عمادة تقنية المعلومات وإدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢٠. سياسة إدارة مخاطر الأمن السيبراني

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لإدارة مخاطر الأمن السيبراني في جامعة الملك فيصل، وذلك وفقاً لاعتبارات سرية الأصول المعلوماتية، والتقنية، وتوافرها، وسلامتها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية وأنظمة وأجهزة التحكم الصناعي الخاصة بجامعة الملك فيصل وإجراءات عمل جامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- البنود العامة

١-١ يجب تطوير وتوثيق واعتماد منهجية إدارة مخاطر الأمن السيبراني (Management Methodology Cybersecurity Risk) وإجراءات إدارة مخاطر الأمن السيبراني في الجامعة ويجب مواءمتها مع الإطار الوطني لمخاطر الأمن السيبراني (National Cybersecurity Risk Management Framework) ويمكن استخدام المعايير والأطر التوجيهية المعتمدة دولياً (مثل: ISO27005، وISO31000، وNIST) في تطوير منهجية إدارة مخاطر الأمن السيبراني.

١-٢ يجب أن تغطي منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يلي:

١-٢-١ تحديد الأصول ومعرفة أهميتها.

١-٢-٢ تحديد وتقييم المخاطر التي تمس أعمال أو أصول أو منسوبي الجامعة (مثل: الآثار المترتبة على جامعة الملك فيصل الناتجة عن المخاطر السيبرانية).

١-٢-٣ تحديد التهديدات والثغرات المتعلقة بالأمن السيبراني التي قد تؤثر على الأصول المعلوماتية والتقنية وتقييمها.

١-٢-٤ تحديد أساليب التعامل مع المخاطر السيبرانية.

١-٢-٥ ترتيب تدابير الحدّ من المخاطر السيبرانية حسب الأولية ووفق إجراءات محدّدة.

١-٢-٦ تصنيف مستويات المخاطر السيبرانية وتعريفها بناءً على مستوى التأثير واحتمالية حدوث التهديد للجامعة.

١-٢-٧ إنشاء سجل مخاطر الأمن السيبراني لتوثيق المخاطر ومتابعتها.

١-٢-٨ تحديد الأدوار والمسؤوليات لإدارة مخاطر الأمن السيبراني والتعامل معها.

١-٣ يجب تنفيذ تقييم المخاطر دورياً لضمان حماية الأصول المعلوماتية والتقنية والتعامل مع المخاطر حسب الأولوية.

١-٤ يجب أن تكون إدارة مخاطر الأمن السيبراني متوافقة مع إدارة المخاطر المؤسسية (Risk Management Enterprise "ERM") في الجامعة.

٢- المراحل الرئيسية لإدارة المخاطر السيبرانية

٢-١ تحديد المخاطر (Risk Identification): يجب أن تُحدّد إدارة الأمن السيبراني الأحداث أو الظروف التي من الممكن أن تنتهك سريّة الأصول المعلوماتية والتقنية وسلامتها وتوافرها، ويشمل ذلك على وجه الخصوص تحديد الأصول المعلوماتية والتقنية، والتهديدات التي من المحتمل أن تتعرّض لها والثغرات ذات الصلة، والضوابط المعتمدة، ومن ثمّ تحديد الآثار الناتجة عن فقدان سريّة هذه الأصول وسلامتها وتوافرها.

٢-٢ تقييم المخاطر (Risk Assessment):

٢-٢-١ يجب على إدارة الأمن السيبراني تنفيذ إجراءات تقييم مخاطر الأمن السيبراني بحد أدنى في الحالات التالية:

٢-٢-١-١ في المراحل الأولى من المشاريع التقنية.

٢-٢-١-٢ قبل إجراء تغيير جوهري في البنية التقنية.

٢-٢-١-٣ عند التخطيط للحصول على خدمات طرف خارجي.

٢-٢-١-٤ عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

٢-٢-٢ يجب إعادة تقييم المخاطر وتحديثها على النحو التالي:

٢-٢-٢-١ دورياً لجميع الأصول المعلوماتية والتقنية، وسنوياً على الأقل للأنظمة الحسّاسة. (CSCC-1-2-1-1)

٢-٢-٢-٢ بعد وقوع حادث متعلّق بالأمن السيبراني ينتهك سلامة الأصول المعلوماتية والتقنية وتوافرها وسريّتها.

٢-٢-٢-٣ بعد الحصول على نتائج تدقيق مهمّة أو معلومات استباقية.

٢-٢-٢-٤ في حال التغيير على الأصول المعلوماتية والتقنية.

٢-٢-٣ يجب أن تغطي عملية تقييم المخاطر ما يلي:

٢-٢-٣-١ تحليل المخاطر (Risk Analysis): يجب أن تُقيّم إدارة الأمن السيبراني احتمالية وقوع التهديدات والآثار الناتجة عنها، وأن تستخدم نتائج هذا التقييم لتحديد المستوى العام لهذه المخاطر. ويجب أن تعتمد إدارة الأمن السيبراني منهجية كميّة (Quantitative) أو نوعيّة (Qualitative) لإجراء تحليل المخاطر.

٢-٣-٢-٢ تقدير المخاطر (Risk Evaluation): يجب أن تُقدِّر إدارة الأمن السيبراني حجم المخاطر السيبرانية بالتوافق مع معايير تقدير المخاطر المؤسسية المعتمدة في الجامعة وتحديد أساليب التعامل معها حسب الأولوية.

٢-٣ معالجة المخاطر (Risk Treatment):

٢-٣-١ يجب أن تحدد إدارة الأمن السيبراني خيارات معالجة المخاطر حسب القائمة التالية:

٢-٣-١-١ معالجة المخاطر أو تقليلها (Risk Mitigation): معالجة أو تقليل درجة الخطر من خلال تطبيق الضوابط الأمنية اللازمة لتقليل احتمال الحدوث أو التأثير أو كليهما، والتي تساعد في احتواء المخاطر والمحافظة عليها ضمن مستويات مقبولة.

٢-٣-١-٢ تجنّب المخاطر (Risk Avoidance): التخلص من الخطر بتجنب الاستمرار بمصدر الخطر.

٢-٣-١-٣ مشاركة المخاطر أو تحويلها (Risk Transfer): مشاركة المخاطر مع طرف ثالث لديه الإمكانيات في التعامل مع المخاطر بشكل أكثر فعالية، أو التأمين على الأصول المعلوماتية والتقنية في حال تعرضها لمخاطر سيبرانية.

٢-٣-١-٤ تقبّل المخاطر وتحمّلها (Risk Acceptance): مستوى الخطر مقبول ولكن يجب المراقبة باستمرار في حال حدوث تغيير.

٢-٣-٢ يجب تحديد خيارات معالجة المخاطر وتوثيقها بناءً على نتائج تقييم المخاطر وتكلفة التنفيذ والمنافع المتوقّعة.

٢-٤ متابعة المخاطر (Risk Oversight):

٢-٤-١ لمتابعة المخاطر يجب أن تُعِدّ إدارة الأمن السيبراني سجلاً للمخاطر وأن تحافظ عليه لتوثيق مخرجات عملية إدارة المخاطر. على أن يشمل بحد أدنى على المعلومات التالية:

٢-٤-١-١ عملية تحديد المخاطر.

٢-٤-١-٢ نطاق المخاطر.

٢-٤-١-٣ المسؤول أو صاحب المخاطر.

٢-٤-١-٤ وصف للمخاطر بما في ذلك أسبابها وآثارها.

٢-٤-١-٥ تحليل للمخاطر يُوضّح التأثيرات الناتجة عن المخاطر ونطاقها الزمني.

٢-٤-١-٦ تقييم وتصنيف للمخاطر يشتمل على احتمالية المخاطر وحجمها وتصنيفها الإجمالي في حال حدوثها.

٢-٤-١-٧ خطّة التعامل مع المخاطر تتضمّن إجراء التعامل معها والشخص المسؤول عنها وجدولها الزمني.

٢-٤-١-٨ وصف الخطر المتبقي.

٢-٤-٢ يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان فعالية إدارة مخاطر الأمن السيبراني.

٢-٤-٣ يجب على إدارة الأمن السيبراني جمع الأدلة المتعلقة بحالة المخاطر السيبرانية ومراجعتها بشكل دوري.

٣- مستوى المخاطر المقبول (Risk Appetite)

٣-١ يجب تحديد معايير تقبّل المخاطر وتوثيقها، وفقاً لمستوى المخاطر وتكلفة معالجة الخطر مقابل تأثيره.

٣-٢ يجب تطبيق ضوابط إضافية من أجل تقليل المخاطر إلى مستوى مقبول في حال عدم استيفاء الخطر المتبقي لمعايير تقبّل المخاطر.

٣-٣ في حال تجاوز معايير تقبّل المخاطر، يتم التصعيد لصاحب الصلاحية لاتخاذ الإجراءات أو القرارات اللازمة.

٤- متطلبات أخرى

٤-١ يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حال حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.

٤-٢ يجب مراجعة سياسة إدارة مخاطر الأمن السيبراني سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢١. سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل على خدمات الحوسبة السحابية والاستضافة Cloud Computing Services and (Hosting). وذلك، لضمان معالجة المخاطر السيبرانية أو تقليلها من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٢-٤ من الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية، وتنطبق هذه السياسة على جميع منسوبي الجامعة.

بنود السياسة

١- **البنود العامة**

١-١ تُطبَق جميع متطلبات الأمن السيبراني الخاصة بالأطراف الخارجية في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية على جميع مقدمي خدمات الحوسبة السحابية والاستضافة.

١-٢ يجب على إدارة الأمن السيبراني التحقق من كفاءة وموثوقية مقدم خدمات الحوسبة السحابية والاستضافة بالإضافة إلى حصوله على ترخيص ووجود سجل رسمي له داخل المملكة العربية السعودية.

١-٣ يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة وفقاً للسياسات والإجراءات التنظيمية الخاصة بالجامعة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٤ يجب على جامعة الملك فيصل إجراء تقييم لمخاطر الأمن السيبراني المترتبة على استضافة التطبيقات أو الخدمات في الحوسبة السحابية قبل اختيار مقدم خدمات الحوسبة السحابية والاستضافة.

١-٥ يجب أن يكون موقع استضافة الأنظمة الحساسة، أو أي جزء من مكوناتها التقنية، داخل الجامعة أو في خدمات الحوسبة السحابية المقدمة من قبل جهة حكومية، أو شركة وطنية محققة لضوابط الهيئة الوطنية للأمن السيبراني المتعلقة بخدمات الحوسبة السحابية والاستضافة، مع مراعاة تصنيف البيانات المستضافة (CSCC-4-2-1-1).

١-٦ يجب على إدارة الأمن السيبراني تطوير وتوثيق واعتماد إجراءات خاصة باستخدام الخدمات السحابية.

١-٧ يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي:

١-٧-١ متطلبات الأمن السيبراني وبنود اتفاقية مستوى الخدمة (Service Level Agreement "SLA").

٢-٧-١ بنود المحافظة على سرية المعلومات (Non-disclosure Clauses) بما في ذلك حذف البيانات وإتلافها بالاتفاق بين مقدم الخدمة والجامعة بناءً على تصنيف تلك البيانات ومع مراعاة سياسة تصنيف البيانات.

٣-٧-١ متطلبات استمرارية الأعمال والتعافي من الكوارث.

٤-٧-١ يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة إمكانية الجامعة إنهاء الخدمة دون مبرر أو اشتراطات.

٨-١ يجب مراجعة تطبيق متطلبات الأمن السيبراني مع مقدمي خدمات الحوسبة السحابية والاستضافة دورياً، مرة واحدة في السنة، على الأقل.

٢- متطلبات الأمن السيبراني المتعلقة باستضافة/تخزين البيانات

١-٢ يجب تصنيف البيانات قبل استضافتها/تخزينها لدى مقدمي خدمات الحوسبة السحابية والاستضافة (ECC-4-2-3-1).

٢-٢ يجب على مقدمي خدمات الحوسبة السحابية والاستضافة إعادة البيانات (بصيغة قابلة للاستخدام) وحذفها بشكل غير قابل للاسترجاع عند إنهاء/انتهاء الخدمة (ECC-4-2-3-1).

٣-٢ يجب أن يكون موقع واستضافة وتخزين معلومات جامعة الملك فيصل داخل المملكة العربية السعودية (ECC-4-2-3-3) مع مراعاة التنظيمات والجوانب التشريعية بعدم خضوع تلك البيانات لأي قوانين دول أخرى.

٤-٢ يجب على إدارة الأمن السيبراني التأكد من فصل البيئة الخاصة بالجامعة (ويشمل ذلك الخوادم الافتراضية، والشبكات وقواعد البيانات) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية (ECC-4-2-3-2).

٥-٢ يجب الحصول على موافقة إدارة الأمن السيبراني لاستضافة الأنظمة الحساسة أو أي جزء من مكوناتها التقنية.

٦-٢ يجب على جامعة الملك فيصل التأكد من تطبيق متطلبات خصوصية البيانات على البيانات المستضافة في الحوسبة السحابية.

٧-٢ يجب تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المخزنة فيها، أو المنقولة منها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة في الجامعة.

٨-٢ يجب على جامعة الملك فيصل التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة يقوم بعمل النسخ الاحتياطي دورياً وحماية النسخ الاحتياطية وفقاً لسياسة النسخ الاحتياطية المعتمدة في الجامعة.

٩-٢ يجب على الجامعة التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة لا يمكنه الاطلاع على البيانات المخزنة وأن صلاحية الوصول الخاصة بمقدم الخدمة محدودة بالصلاحيات اللازمة للقيام بأنشطة إدارة خدمة الاستضافة وصيانتها، أو حسب متطلبات الأعمال.

٢-١٠ يجب على مقدم خدمات الحوسبة السحابية والاستضافة تقييد الدخول إلى الخدمات السحابية الخاصة بالجامعة على المستخدمين المصرح لهم فقط وباستخدام وسائل التحقق من هوية المستخدم وفقاً لسياسة إدارة هويات الدخول والصلاحيات المعتمدة في الجامعة.

٢-١١ يجب على مقدم خدمات الحوسبة السحابية والاستضافة توفير التقنيات والأدوات اللازمة للجامعة لإدارة ومراقبة خدماتها السحابية.

٢-١٢ يجب على إدارة الأمن السيبراني ومكتب إدارة المشاريع بعمادة تقنية المعلومات التنسيق والتعاون مع الجهة المعنية بالشؤون القانونية في الجامعة من أجل تضمين بنود متطلبات الأمن السيبراني المتعلقة باستضافة البيانات في العقد مع مقدم خدمة الحوسبة السحابية.

٣- متطلبات أخرى

٣-١ يجب التأكد من تفعيل سجلات الأحداث على الأصول المعلوماتية المستضافة.

٣-٢ يجب مراقبة سجلات الأحداث الخاصة بالأمن السيبراني دورياً.

٣-٣ يجب التأكد من مزامنة التوقيت (Clock Synchronization) الخاص بالبنية التحتية للخدمة السحابية مع التوقيت الخاص بالجامعة.

٣-٤ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية الأصول المعلوماتية والتقنية على خدمات الحوسبة السحابية.

٣-٥ يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دورياً.

٣-٦ يجب مراجعة هذه السياسة مرة واحدة في السنة على الأقل.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ وتطبيق السياسة:** الأقسام ذات العلاقة في عمادة تقنية المعلومات وإدارة الأمن السيبراني.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.

- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢٢. سياسة النسخ الاحتياطي

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بضمان حماية البيانات والمعلومات والإعدادات التقنية للأنظمة والتطبيقات الخاصة بجامعة الملك فيصل من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية لجامعة الملك فيصل والمتطلبات التشريعية والتنظيمية ذات العلاقة. بالإضافة إلى توفير إطار متسق لتطبيقه على عملية النسخ الاحتياطي للمساعدة في منع حدوث فقد في بيانات جامعة الملك فيصل من خلال ضمان توفر نسخ احتياطية من البيانات تعمل بشكل صحيح عند الحاجة إليها، سواء كان ذلك لمجرد استرداد ملف معين أو عند الحاجة إلى الاسترداد الكامل لأنظمة التشغيل وأنظمة التطبيقات الخاصة بالجامعة.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٩ إدارة النسخ الاحتياطية (Backup and Recovery Management) من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع إجراءات وعمليات إدارة النسخ الاحتياطية لأنظمة وبيانات جامعة الملك فيصل، وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

١- البنود العامة

١-١ يجب أن تغطي متطلبات الأمن السيبراني المتطلبات والضوابط الأساسية لإدارة النسخ الاحتياطية (ECC-2-9-3) بحد أدنى ما يلي:

* نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة.
* القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني.

١-٢ يجب أن تغطي إدارة النسخ الاحتياطية متطلبات وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC: 2019) وذلك بحد أدنى ما يلي:

* نطاق عمل النسخ الاحتياطي المتصل وغير المتصل (Backup Offline and Online) ليشمل جميع الأنظمة الحساسة بما فيها البيانات والمعلومات والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجامعة.
* عمل النسخ الاحتياطي على فترات زمنية مخطط لها بناءً على تقييم المخاطر، كما يُوصى بعمل النسخ الاحتياطي للأنظمة الحساسة بشكل يومي.

* تأمين الوصول والتخزين والنقل لمحتوى النسخ الاحتياطية للأنظمة الحساسة ووسائطها وحمايتها من الإتلاف أو التعديل أو الاطلاع غير المصرح به.

* إجراء فحص دوري كل ثلاثة أشهر على الأقل لتحديد مدى فعالية استعادة النسخ الاحتياطية الخاصة بالأنظمة الحساسة.

١-٣ يجب مراجعة تطبيق المتطلبات التنظيمية ذات العلاقة بالأمن السيبراني لإدارة النسخ الاحتياطية.

١-٤ يجب تحديد البيانات الأكثر أهمية للقطاعات الرئيسية بالجامعة وذلك من خلال عملية تصنيف البيانات ومن خلال مراجعة أصول المعلومات، حيث يجب تحديد البيانات الهامة والحرجة بحيث يمكن منحها أولوية أعلى أثناء عملية النسخ الاحتياطي.

١-٥ يجب الاحتفاظ بنسخة احتياطية من:

* جميع البيانات التي تقرر الجامعة أنها هامة وحساسة للأعمال والأنشطة الرئيسية لقطاعات الجامعة و/أو حسب طبيعة ومهام الموظف.

* جميع البيانات المخزنة على خوادم الملفات أو خدمة مشاركة البيانات التابعة للجامعة بحيث تكون مسؤولية الموظف نقل بياناته الهامة إلى موقع التخزين الشبكي.

* جميع البيانات المخزنة على خوادم الشبكة، والتي قد تتضمن خوادم الويب وخوادم قواعد البيانات ووحدات التحكم في أنظمة المجال الجامعي KFU Domain وأنظمة الجدار الناري وخوادم الوصول عن بُعد.

١-٦ يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية.

٢- تخزين النسخ الاحتياطي

٢-١ يجب أن تُخزن وسائط النسخ الاحتياطي في حاوية مقاومة للحريق وفي منطقة مؤمنة بأنظمة التحكم بالدخول ويتم مراقبتها بأنظمة المراقبة الأمنية بالكاميرات.

٢-٢ يجب الحفاظ على الفصل الجغرافي بين أماكن حفظ النسخ الاحتياطية وموقع مركز بيانات الجامعة، بمسافة مناسبة وذلك للحماية من الحرائق أو الفيضانات أو الكوارث الطبيعية الأخرى، وذلك حفاظاً على عدم حدوث أي ضرر في حالة حدوث كارثة في الموقع الرئيسي لمركز البيانات.

٢-٣ عند نقل وسائط النسخ الاحتياطي أو حفظها خارج الموقع الرئيسي لمركز البيانات فإنه يجب ضمان -وبشكل معقول- عدم تعرضها للكوارث كالسرقة أو الحرائق، كما يجب اختيار أماكن تخزين تستخدم أساليب حماية من الكوارث البيئية وتخضع للتحكم في الوصول لضمان سلامة وسائط النسخ الاحتياطي.

٣- تكرار النسخ الاحتياطي

٣-١ يجب إجراء عملية النسخ الاحتياطي على فترات منتظمة.

٢-٣ الآلية التي يتم بها تكرار عملية النسخ الاحتياطي هي ما يضمن استعادة البيانات بنجاح، ويجب جدولة مواعيد مناسبة لعملية النسخ الاحتياطي بحيث تكون متوافقة مع طبيعة عمل قطاعات الجامعة وبحيث يمكن استعادة البيانات الكافية لاستمرار العمل في حالة وقوع حادث مفاجئ، وذلك لكي يمكن تجنب ضغط العمل على المستخدمين وعلى مسؤول النسخ الاحتياطي.

٣-٣ يجب التعريف والتوعية لكافة منسوبي الجامعة بأن كلاً منهم مسؤول بصورة شخصية عن بياناته الموجودة على أجهزة سطح المكتب أو أجهزة الحاسب المحمول التي في عهدتهم، ويقع على عاتقهم مسؤولية تخزين جميع البيانات المهمة الموجودة لديهم على خدمات النسخ الاحتياطي ومشاركة الملفات المعمول بها في الجامعة.

٤-٣ يجب تحديد المستوى الذي تكون عنده المعلومات ضرورية ويتعين تخزين نسخ احتياطية لها.

٥-٣ يجب اختبار وتوثيق إجراءات استعادة البيانات، مع تحديد من هو المسؤول عن عملية استعادة البيانات وكيف يتم تنفيذها وتحت أي ظروف يجب تنفيذها والمدة التي تستغرقها كامل العملية بدءاً من الطلب وانتهاءً باستعادة البيانات، ويجب أن تكون تلك الإجراءات واضحة وموجزة بحيث لا تكون مربكة ويساء تفسيرها في وقت الأزمات من قِبل المستخدمين بخلاف مسؤولي النسخ الاحتياطي.

٤- الاحتفاظ بالنسخ الاحتياطي

١-٤ يجب تحديد الوقت اللازم للاحتفاظ بالنسخ الاحتياطي، وما هو عدد النسخ المخزنة من البيانات المنسوخة احتياطياً الكافية للحد من المخاطر بكفاءة مع الحفاظ على البيانات المطلوبة.

٢-٤ يجب الاحتفاظ بنسخ احتياطية وفقاً لجدول الحفظ والتخلص من النسخ الاحتياطي، ويحدد هذا الجدول حالة البيانات فيما إذا كان يمكن التخلص منها أو إعادة تدويرها أو إبقاؤها في مخزن الأرشيف.

٥- النسخ المخزنة

١-٥ النسخ المخزنة يجب أن تخزن مع وصف قصير يتضمن المعلومات التالية:

١-١-٥ تاريخ النسخ الاحتياطي / اسم المؤرِد / نوع طريقة النسخ الاحتياطي (كامل / تزايدي).

٢-١-٥ يجب الاحتفاظ بسجل للحركات المادية والإلكترونية لجميع النسخ الاحتياطية، ويجب أن تشير الحركة المادية والإلكترونية للنسخ الاحتياطية إلى:

* النسخة الاحتياطية الأولية وطريقة نقلها إلى التخزين.
* أي حركة للنسخ الاحتياطية من موقع التخزين الخاص بها إلى موقع آخر.

٢-٥ يجب توفير النسخ المخزنة فور ورود طلب معتمد، ويجب أن تتم الموافقة على طلب البيانات المخزنة من قبل شخص مخول له، ويقوم بترشيحه رئيس قسم الشبكات ونظم التشغيل بعمادة تقنية المعلومات، كما يجب أن تتضمن طلبات البيانات المخزنة ما يلي:

* تعبئة نموذج يوضح تفاصيل الطلب، بما في ذلك النسخة المطلوبة وأين ومتى يرغب مقدم الطلب في استلامها والغرض من طلب النسخة.
* الإقرار بأن النسخة الاحتياطية سيتم إرجاعها أو إتلافها فور الانتهاء من استخدامها.
* تقديم إيصال تسليم كدليل على أن النسخة الاحتياطية قد تم إرجاعها.

٣-٥ يجب توفير مستوى حماية مناسب للمعلومات المخزنة في موقع التخزين الاحتياطي وفقاً للمعايير المطبقة في الموقع الرئيسي لمركز البيانات، كما ينبغي أن تمتد الضوابط المطبقة على وسائط النسخ الاحتياطي في الموقع الرئيسي لمركز البيانات لتشمل موقع التخزين الاحتياطي.

٦- اختبار عملية استعادة البيانات

٦-١ يجب أن يتم الفحص والقيام بإجراءات استعادة النسخ الاحتياطية بشكل منتظم لضمان فعاليتها وللتحقق من إمكانية استكمال اجراءات عملية الاستعادة في الوقت المحدد والإبلاغ عن قدرتها على استعادة البيانات.

٦-٢ يجب اختبار وسائط النسخ الاحتياطي بانتظام لضمان الاعتماد عليها للاستخدام الطارئ عند الضرورة.

٦-٣ يجب اختبار استعادة النسخ الاحتياطي عند إجراء أي تغيير قد يؤثر على نظام النسخ الاحتياطي.

٦-٤ يجب مراجعة معلومات سجل الأحداث الناتجة من كل مهمة نسخ احتياطي يومياً للأغراض التالية:

* للتحقق من الأخطاء وتصحيحها.
* لمراقبة مدة عملية النسخ الاحتياطي.
* لتحسين أداء النسخ الاحتياطي حيثما أمكن ذلك.

٧- وسائط النسخ الاحتياطي

يجب حماية وسائط النسخ الاحتياطي من الوصول غير المصرح به أو سوء الاستخدام أو العبث بها، بما في ذلك الحماية الكافية لتجنب أي ضرر مادي ينشأ أثناء عملية نقلها أو تخزينها. لذا يجب على جميع الموظفين المسؤولين عن معالجة النسخ الاحتياطي للبيانات إثبات الهوية والحصول على إذن بمعالجة تلك النسخ الاحتياطية.

٧-١ عند الحاجة إلى ضوابط خاصة لحماية المعلومات السرية أو الحساسة، ينبغي مراعاة ما يلي:

* استخدام أماكن تخزين (خزانة) آمنة.
* التسليم باليد.
* في الحالات الحرجة يتم تقسيم ما سيتم تسليمه إلى أجزاء يرسل كل جزء عبر وسيلة مختلفة عن غيرها.

٧-٢ يجب التخلص من جميع وسائط النسخ الاحتياطية بشكل مناسب، وذلك كما يلي:

* يجب تجهيز وسائط النسخ الاحتياطي للتخلص منها.

* يجب ألا تحتوي الوسائط على نسخ احتياطية (فعالة) بحيث يمكن إعادة استخدامها.
* يجب ضمان عدم الوصول لمحتويات الوسائط الحالية أو السابقة وقراءتها أو استرجاعها من قبل طرف غير مصرح له.
* يجب العمل على أن تتلف وسائط النسخ الاحتياطي مادياً بحيث لا يمكن استعادة محتوياتها قبل التخلص منها.

٣-٧ حيث إن هناك أنواعاً معينة من وسائط النسخ الاحتياطي لها عمر وظيفي محدود إذ أنه بعد مدة معينة من الخدمة لن يكون بالإمكان اعتبار هذه الوسائط موثوقاً بها عند وضعها في الخدمة، لذلك فإنه يجب تسجيل التاريخ عليها ليتم إيقافها عن الخدمة بعد أن يتجاوز وقت استخدامها مواصفات المصنع.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني والأقسام ذات العلاقة في عمادة تقنية المعلومات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢٣. سياسة حماية وتصنيف البيانات والمعلومات

الأهداف

الغرض من هذه السياسة هو حماية البيانات، البيانات المخزنة (الإلكترونية أو السجلات الورقية) التي تحتفظ بها جامعة الملك فيصل، وكذلك الأشخاص الذين يستخدمونها والطرق التي يتبعونها في التعامل بها والأجهزة المستخدمة للوصول إليها، لضمان حماية السرية وسلامة بيانات ومعلومات الجامعة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما تقوم هذه السياسة بتحديد المتطلبات والمسؤوليات الأساسية للإدارة السليمة لأصول البيانات وتحديد وسائل التعامل مع البيانات ونقلها داخل الجامعة.

كما تصف السياسة المبادئ التي يجب اتباعها لحماية المعلومات، وذلك من خلال تحديد كيف ولمن يمكنك نشر هذه المعلومات بتصنيف معين من أجل الحفاظ على خصوصية وسلامة وتوفر أصول المعلومات بالجامعة. بالإضافة إلى تحديد متطلبات التعامل مع بيانات الجامعة من أجل توفير أساسيات لحمايتها.

نطاق العمل وقابلية التطبيق

تسري هذه السياسة على جميع من يقوم بالأعمال من النظم والأشخاص وطرق العمل، ويشمل ذلك جميع المدراء التنفيذيين واللجان والإدارات والشركاء والموظفين والأطراف الأخرى الذين لديهم إمكانية الوصول إلى نظم المعلومات أو البيانات التي يتم إنشاؤها أو جمعها أو تخزينها أو معالجتها في جامعة الملك فيصل، سواء كانت في شكل إلكتروني أو غير إلكتروني، وبصرف النظر عن مكان وجود هذه البيانات أو نوع الجهاز المخزنة به، وبالتالي ينبغي أن يستخدمها جميع الموظفين، والأطراف الأخرى التي تتعامل مع البيانات التي تحتفظ بها الجامعة أو تخصها.

بنود السياسة

١- البنود العامة

١-١ يجب التعامل مع المعلومات حسب التصنيف المحدد بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

١-٢ يجب تطبيق متطلبات الامن السيبراني لحماية البيانات ومعلومات الجامعة.

١-٣ يجب تصنيف بيانات ومعلومات الجامعة الموجودة في الأنظمة الحسّاسة والتي تُعالجها الأطراف الخارجية وفقاً لوثيقة ضوابط الأنظمة الحساسة الصادرة من الهيئة الوطنية للأمن السيبراني (CSCC-2-6-1-2).

١-٤ يجب استخدام تقنيات حماية البيانات والمعلومات في تطبيقات الويب الخارجية.

١-٥ يجب استخدام التحقق من هوية المستخدم لنقل البيانات السرية للغاية إلى أطراف خارجية باستخدام شهادات التشفير الرقمية (Digital Certificates) المعتمدة.

١-٦ يجب تصنيف مفاتيح التشفير الخاصة باعتبارها معلومات "سرية للغاية".

١-٧ في جميع الحالات يجب الرجوع إلى ضوابط المركز الوطني للوثائق والمحفوظات فيما يخص أعمال الأرشفة وحفظ وإتلاف الوثائق.

١-٨ يجب تطبيق تصنيف جميع بيانات جامعة الملك فيصل وفقا لسياسة التصنيف المعتمدة من مكتب إدارة البيانات في الجامعة. (الملاحق ص ٢٥٠)

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني ومكتب إدارة البيانات ودعم اتخاذ القرار وجميع جهات الجامعة.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢٤. سياسة الأمن المادي والبيئي

الأهداف

الغرض من هذه السياسة هو تحديد القواعد الأساسية لمنع الدخول غير المصرح به والتداخل مع مرافق وأنظمة أمن المعلومات لدى جامعة الملك فيصل وكذلك الحفاظ على أمن المعلومات والموظفين من التعرض إلى التهديدات المادية المختلفة، والتي من شأنها التأثير بشكل سلبي على الأنظمة الإلكترونية والخدمات الرقمية أو توقفها عن العمل، وذلك لضمان حماية الأصول المعلوماتية والتقنية للجامعة من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٤ الأمن المادي (Physical Security) من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تنطبق هذه السياسة على منسوبي جامعة الملك فيصل وأي طرف ثالث سواءً كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم، وتغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

بنود السياسة

١- **ضوابط الأمن المادي القائمة على المخاطر**

* يجب أن تتأكد الجامعة من أن جميع منشآتها المادية تتمتع بعوامل الأمان بما يتوافق مع مخاطر أنظمة المعلومات في تلك المنشآت.
* يتم تحديد جميع المنشآت المادية لدى الجامعة وتعين تصنيف أمني لها.
* يتم تخطيط الأمن المادي والبيئي للمنشآت المادية لدى الجامعة مع الأخذ بعين الاعتبار درجة تصنيف أمن المعلومات والمعايير المتعلقة بالنوع المحدد من البنية التحتية المادية لدى الجامعة.
* تُعنى إدارة الأمن والسلامة في الجامعة بمسؤولية التأكد من تطبيق ضوابط الأمن المادي للمباني والمنشآت.

٢- **المناطق الآمنة**

* يجب أن تقوم الجامعة بتطوير مخطط الأمن المادي لمرافقها كما يجب توزيع المخطط المادي الخاص بالجامعة على مناطق بحيث يكون لكل منطقة مستوى أعلى من القيود التي تحكم متطلبات التصريح بالدخول، ويمكن تصنيف المناطق المحيطية كالتالي:
  - المنطقة العامة ومنطقة الاستقبال: (قيود محدودة وتخضع هذه المنطقة للمراقبة العامة).

- منطقة المكاتب: (دخول محدود، يتم تسجيل الدخول ومرافقة الزوار الذين يدخلون إلى هذه المنطقة، كما تخضع المنطقة للمراقبة العامة).
- منطقة الدخول الآمنة: (دخول محدود، يتم تسجيل الدخول ومرافقة دخول الزوار، وتخضع المنطقة للإشراف)
- منطقة الدخول المقيد: (التي تقتصر على دخول الأشخاص المصرح لهم فقط) ويخضع الدخول لقيود عالية، ويتم تسجيل الدخول، ويجب حصول الموظفين والزوار الذين يدخلون إلى هذه المنطقة على تصريح محدد بالدخول، كما تخضع هذه المنطقة للمراقبة.
- يجب التأكد من أن مرافق معالجة المعلومات لا تقع في منطقة غير مستقرة من ناحية البيئة.
- يجب التأكد من عدم وقوع مرافق معالجة المعلومات على مقربة من أي مرافق مجاورة خطرة (مثل المختبرات الكيميائية وخلافه).
- يجب التأكد من تخزين المعدات المزمع استخدامها في الحالات الطارئة ووسائط النسخ المساندة على مسافة آمنة بعيداً عن الموقع الرئيسي لتفادي التعرض لنفس الطوارئ التي تتحدث في الموقع الرئيسي.

٣- التحكم بالدخول المادي

* يسمح لموظفي وموردي ومقاولي الجامعة بالدخول إلى المرافق المادية لدى الجامعة بما في ذلك مرافق معالجة المعلومات، وذلك فقط بناءً على التعريف بأنفسهم والتحقق من هويتهم وفقاً لإجراءات منح صلاحية الدخول المادي.

* يتم اعتماد الوصول إلى المناطق الآمنة والمقيدة من قبل المسؤول عن النشاط / تقنية المعلومات. ويكون الدخول إلى المناطق التي تتمتع بتصنيف أمني مرتفع مثل مركز البيانات محصوراً على الأشخاص الذين لديهم مسؤولية مباشرة عن تشغيل وصيانة مركز البيانات.

* يجب أن يُطلب من موظفي وموردي ومقاولي الجامعة والزوار الآخرين أن يضعوا شارة تعريفية فريدة أثناء تواجدهم في مرافق الجامعة بشكل دائم.

* ينبغي أن يوقع كل زائر على سجل الزوار الذي يتم الاحتفاظ به لزوار الجامعة. يجب أن يتم توثيق اسم الزائر وشركته والغرض من الزيارة ووقت الدخول ووقت المغادرة والتاريخ في ذلك السجل.

* يمنع منعاً باتاً مشاركة الموظفين بعضهم باستخدام بطاقة الدخول إلى منشآت العمل.

* يجب عدم وضع أدلة الهاتف والوثائق الداخلية المستخدمة في تحديد مواقع مرافق المعالجة الحساسة في مكان يسهل الوصول إليها من قبل الموظفين الداخليين والخارجيين الذي ليست لديهم الصلاحيات الأمنية المطلوبة.

* يجب مرافقة جميع الزوار أثناء تجوالهم في المناطق الآمنة من قبل موظفي الجامعة.

٤- فحص مواد أمن المعلومات /والمواد الداخلة إلى والخارجة من المناطق الآمنة

* يتعين القيام بتفتيش المواد الداخلة إلى والخارجة من الجامعة قبل نقلها من مناطق الدخول العامة إلى نقطة استخدامه.

* يجب أن يتم التصريح رسمياً بجميع طلبات النقل من قبل المسؤول عن المعلومات وتسجيلها من قبل موظفي الأمن المادي.

٥- **صيانة البنية التحتية للأمن المادي والبيئي**

* يتعين على الجامعة التفويض بمراقبة والتحكم بأي أنشطة صيانة وأنشطة تشخيصية يتم تنفيذها محلياً أو عن بعد.

* يجب مراقبة كافة عمليات الصيانة وعلى موظفي الجامعة المعنيين مراجعة سجلات الصيانة.

٦- **الحماية من الحريق**

* تضطلع إدارة الأمن والسلامة بمسؤولية الاستجابة لحوادث الحريق الطارئة وإجراء تمارين للتعامل مع الحريق.

* ينبغي إجراء تمارين التعامل مع الحريق بشكل ربع سنوي. كما ينبغي مراقبة تلك التمارين، وتزويد جميع المشاركين بإفادات تتعلق بمساهمتهم وأدائهم.

* تقوم إدارة الأمن والسلامة بتحديد المواقع الحرجة التي سيتم تجهيزها بطفايات حريق يدوية. وعليه فإنه يتعين وضع بطاقات واضحة على تلك المناطق والتبليغ عن موقعها بشكل دوري لجميع الموظفين أثناء التدريب التوعوي واستخدام النشرات الموجزة.

* تجهيز أبواب مخارج الحريق لتفتح من الداخل فقط، كما ينبغي إعداد إنذارات الحريق لتنطلق فوراً عند فتح مخرج الطوارئ، وذلك كجزء من تدابير الأمن المادي المطلوبة أثناء الإخلاء بسبب الحريق.

٧- **مراقبة الأمن المادي والبيئي**

* يجب أن تتأكد الجامعة من مراقبة ضوابط الأمن المادي والبيئي لديها بما يتوافق مع مستويات تصنيف المخاطر لبيئة الأمن المادي ذات العلاقة.

* تقوم إدارة الأمن والسلامة بتطوير خطة مراقبة الأمن المادي والبيئي المبنية على المخاطر، والتي تحدد ضوابط الأمن المادي والبيئي الواجب مراقبتها والمسؤوليات التي سيتم تحديدها بهذا الصدد.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني والأقسام ذات العلاقة في عمادة تقنية المعلومات وإدارة الأمن وإدارة السلامة.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.

- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢٥. سياسة إدارة الأصول

الأهداف

الغرض من هذه السياسة هو التأكد من أن جامعة الملك فيصل لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة بالجامعة، من أجل دعم العمليات التشغيلية للجامعة ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها ودقتها وتوافرها ، بالإضافة إلى التأكد من أن أنظمة المعلومات لدى الجامعة قد تم تحديدها وتعيين مسؤولين محددين عنها، وتصنيفها بشكل مناسب بما يتوافق مع طبيعة هذه الأنظمة وتصنيف مخاطر أمن المعلومات المتعلقة بها، مما يساعد على تحديد الضوابط الأمنية المناسبة لها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١ إدارة الأصول (Asset Management) من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم جامعة الملك فيصل بتشغيلها أو قد تعاقدت الجامعة على تشغيلها مع طرف ثالث، وتنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.

بنود السياسة

١- البنود العامة

* يجب التعامل مع المعلومات حسب التصنيف المحدد بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.
* يجب تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية.
* يجب تحديد وتوثيق واعتماد ونشر سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية.
* يجب تطبيق سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية.
* يجب تصنيف الأصول المعلوماتية والتقنية للجهة وترميزها (Labeling) والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
* يجب مراجعة متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية دورياً.
* يجب تصنيف بيانات ومعلومات الجامعة الموجودة في الأنظمة الحسّاسة والتي تُعالجها الأطراف الخارجية - وفقاً لضوابط الأنظمة الحساسة (CSCC-2-6-1-2).
* يجب استخدام تقنيات حماية البيانات والمعلومات في تطبيقات الويب الخارجية الخاصة بالجامعة.

* يجب استخدام التحقق من هوية المستخدم لنقل البيانات السرية للغاية إلى أطراف خارجية باستخدام شهادات التشفير الرقمية (Digital Certificates) المعتمدة في الجامعة.
* يجب تصنيف مفاتيح التشفير الخاصة باعتبارها معلومات "سرية للغاية"

٢- تعريف أنظمة المعلومات

* تعرِّف أنظمة المعلومات على أنها البنية التحتية التقنية والطبيعية التي تؤثر بصورة مباشرة أو غير مباشرة على تحديد ومعالجة وتبليغ وتدمير وتخزين معلومات الجامعة، ويشمل ذلك ما يلي:
  - البرامج التطبيقية لتقنية المعلومات.
  - البنية التحتية التقنية لمعالجة المعلومات (أجهزة الحاسوب وأجهزة معالجة المعلومات الأخرى مثل مقاسم الاتصالات والهواتف الذكية، الطابعات، وغير ذلك).
  - البنية التحتية للشبكة والأمن.
  - البنية التحتية المادية (المباني، المكاتب، غرف الاجتماعات، وخلافه).
  - الوثائق.
  - عناصر البنية التحتية الأخرى ذات العلاقة.

٣- تحديد أنظمة المعلومات

يجب تحديد جميع أنظمة المعلومات لدى الجامعة من خلال إجراء جرد لتلك الأنظمة من قبل إدارة تقنية المعلومات وإدارة أمن المعلومات وفقاً لإجراءات تحديد أنظمة المعلومات (مع ملاحظة أن المعلومات التي تم تجميعها في سجلات أنظمة المعلومات يجب دمجها في هذا الجرد لأنظمة المعلومات).

٤- تصنيف أنظمة المعلومات

يجب تعيين درجة تصنيف لكل نظام من أنظمة معلومات الجامعة، مع الأخذ في الاعتبار الأثر المتوقع على نشاط الجامعة في حال انتهاك سرية أو سلامة أو توفر نظام المعلومات.

يجب على المسؤول عن نظام المعلومات بتصنيف أنظمة المعلومات طبقاً لتصنيف أنظمة معلومات الجامعة، وذلك وفقاً لإجراءات تصنيف أنظمة المعلومات.

٥- وضع بطاقات تعريفية على أنظمة المعلومات

يجب أن يتم وضع بطاقات على كل نظام من أنظمة المعلومات المادية من قبل مسؤول ذلك النظام.

٦- المسؤولون والراعون لأنظمة المعلومات

المسؤول عن نظام المعلومات هو الشخص أو الإدارة الذين تكون لهم المسؤولية النهائية ولديهم الصلاحيات المتعلقة بنظام المعلومات، ويقررون كيف ومن سيستخدم النظام.

راعي نظام المعلومات هو الشخص أو الإدارة الذين تم تكليفهم بالمسؤولية عن إدارة عمليات، وتغييرات، وصيانة، والتخلص من نظام المعلومات بتفويض من المسؤول عن المعلومات.

يضطلع المسؤول عن نظام المعلومات بالمسؤولية النهائية عن أمن ذلك النظام.

يضطلع راعي نظام أمن المعلومات بالاشتراك مع إدارة أمن المعلومات بمسؤولية تطبيق الضوابط المطلوبة لتوفير عوامل الأمان لذلك النظام.

٧- **تحديث جرد أنظمة المعلومات**

يجب أن يتم مراجعة جرد أنظمة المعلومات بشكل منتظم وتحديثها إذا اقتضى الأمر وفقاً لإجراءات مراجعة وتحديث جرد أنظمة المعلومات المعمول بها في الجامعة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني والأقسام ذات العلاقة في عمادة تقنية المعلومات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢٦. سياسة أمن المشتريات

نطاق العمل وقابلية التطبيق

تسعى الجامعة إلى الاستفادة من مستوى النضج المتحقق في عملية الأتمتة وبالتالي تقليل التكاليف التشغيلية المرتبطة بعمليات المعاملات المالية الإدارية، مع زيادة الدعم الفني للأنظمة على مستوى كافة الإدارات بالجامعة. إن دور الأمن السيبراني فيما يخص عملية الشراء هو جزء لا يتجزأ من حماية البيانات الحساسة على مستوى قطاعات الجامعة، مستنداً في ذلك على الاستجابة من خلال تخفيف المخاطر التي قد تنتج من عمليات سلسلة التوريدات والإمدادات.

بنود السياسة

يجب تأمين كافة الجوانب المتعلقة بالمخاطر المحتملة لخرق بيانات أنظمة وقواعد البيانات.

يجب أن تعمل إدارة المشتريات والمناقصات وكذلك الإدارة العامة للشؤون الإدارية والمالية وكافة الإدارات الأخرى بالجامعة المتعاملة على النظام المالي والإداري على تحديد أنواع المعلومات التي ستديرها في النظام المالي والإداري، بحيث يتم تحديد صلاحيات من سيصل إلى النظام، ومن أي موقع سيصل إليه. ومن خلال القيام بذلك سيكون لدى الفريق فهم أفضل للمخاطر المحتملة.

يجب كذلك التأكد من تشفير جميع البيانات المنقولة بين التطبيقات المتصلة معًا والتي منها النظام المالي والإداري.

يجب التأكد من أن أي خدمة قائمة على مبدأ الحوسبة السحابية فإنه يتم اتخاذ إجراءات وقائية حيالها لأمن الشبكات مثل استخدام اعدادات أمنية على أجهزة جدار الحماية.

بالإضافة إلى ذلك فإنه يجب أن يتم التأكد من أن ضوابط الأمان والحماية متوفرة بالنظام المالي والإداري والتأكد من تأمينه وحمايته من هجمات رفض الخدمة الموزع (DDoS) الذي يمكن أن يؤدي إلى انقطاع الخدمة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني والأقسام ذات العلاقة في عمادة تقنية المعلومات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢٧. سياسة عدم إفشاء المعلومات:

نطاق العمل وقابلية التطبيق

إن عدم التزام منسوبي الجامعة بتطبيق سياسة عدم إفشاء المعلومات يعتبر بمثابة كشفًا عن معلومات الجامعة التي قد تكون مصنفة حسب درجة سريتها، ويجب أن يعتبر هذا بمثابة حادثًا سيرانيًا لتسريب المعلومات أو البيانات الخاصة بالجهات الحكومية ويجب التعامل معه وفقًا لذلك. وفي حال انتهاك السرية وعدم الامتثال لاتفاقيات عدم الكشف فإنه يجب إبلاغ إدارة الأمن السيبراني في أقرب وقت ممكن. ويجب أن يتم إتاحة نموذج اتفاقية عدم الإفشاء NDA على البوابة الإلكترونية للجامعة للعمل بموجبه.

بنود السياسة

يجب أن يكون كل اتصال مع الجهات الحكومية أو السلطات التنظيمية من خلال الاستناد إلى سياسة الاتصال والتواصل المعمول بها في الجامعة.

ويجب أن يكون الموظف مخولًا من قبل رئيسه في العمل لكي يقوم بعملية الاتصال الخارجي.

يجب كذلك على جميع الموظفين المرور من خلال رئيس القسم أو مسؤول الجهة لمعرفة آلية الاتصال الموافق عليها ويجب وضع وبروتوكول محدد لمثل هذا النوع من الاتصالات الخارجية.

فيما يتعلق بأمن المعلومات، فإن جميع الاتصالات مع الجهات الخارجية والخاصة يجب أن تكون بإذن من قِبل المسؤول على إدارة الأمن السيبراني بالجامعة أو من يفوضه صاحب الصلاحية معالي رئيس الجامعة، وذلك على أساس كل حالة على حدة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني والأقسام ذات العلاقة في عمادة تقنية المعلومات.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢٨. سياسة الخصوصية

مقدمة

تتمثل رؤية البوابة الإلكترونية لجامعة الملك فيصل في سعي الجامعة لأن تصبح بوابتها الإلكترونية نافذة عملية للتعرف على أنشطة وخدمات الجامعة، كونها بيئة مناسبة لنشر المعرفة وحقلًا لتبادل الخبرات على المستويين الإقليمي والدولي الأمر الذي من شأنه أن يثري العملية التعليمية قدماً الى الامام. ولأن إدارة البوابة معنية ببذل قصارى جهدها لتقديم خدمة ذات جودة عالية لكل المستفيدين، فهي تضع سرية معلوماتهم على رأس قائمة الأولويات. وبالتالي حددت الإدارة عدداً من المبادئ الواجب مراعاتها من قِبل مستخدم البوابة من أجل الحفاظ على خصوصية وسرية معلوماته، علماً بأن تلك المبادئ تشكل فيما بينها سياسة للخصوصية وسرية المعلومات. وعلى زوار البوابة الاطلاع المستمر على سياسة الخصوصية وما تحويه من شروط ومبادئ لضمان سرية المعلومات من أجل التعرف على أية تحديثات تتم عليها، علماً بأن إدارة البوابة غير مطالبة بالإعلان عن أية تحديثات تتم على تلك الشروط والمبادئ. ويعني استخدامك للبوابة أنك اطلعت ووافقت على تلك الشروط والمبادئ وما يتم عليها من تعديلات مستمرة.

نطاق العمل وقابلية التطبيق

تم إعداد سياسة الخصوصية لمساعدة الزوار والمستخدمين على تفهم طبيعة البيانات التي يتم جمعها منهم عند زيارة البوابة وكيفية التعامل معها.

تتخذ البوابة الإلكترونية للجامعة الإجراءات والتدابير المناسبة والملائمة للحفاظ على المعلومات الشخصية التي لديها وحفظها بشكل آمن بما يضمن حمايتها من الفقدان أو الدخول غير المصرح به أو إساءة الاستخدام، أو التعديل والإفصاح غير المصرح بهما، ومن أهم التدابير المعمول بها في إدارة البوابة لحماية معلومات الزائر الشخصية ما يلي:

- الإجراءات والتدابير المشددة لحماية أمن المعلومات والتقنيات المستخدمة للوقاية من عمليات الاحتيال والدخول غير المصرح به إلى أنظمتنا.
- التحديث المستمر لإجراءات وضوابط الحماية التي تفي أو تزيد عن المعايير القياسية.
- تأهيل الموظفين المسؤولين عن إدارة البوابة وتدريبهم على احترام سرية المعلومات الشخصية لزوار البوابة وزائراتها.

بنود السياسة

* جمع المعلومات

- بمجرد زيارة المستخدم للبوابة الإلكترونية للجامعة، يقوم خادم خاص بتسجيل عنوان بروتوكول شبكة الإنترنت IP الخاص بالمستخدم، بالإضافة إلى تاريخ ووقت الزيارة والعنوان URL الخاص بأي موقع إلكتروني يتم من خلاله توجيه المستخدم إلى البوابة الإلكترونية للجامعة.
- تضع معظم المواقع الإلكترونية بمجرد أن تتم زيارتها ملفاً صغيراً على القرص الصلب الخاص بجهاز الزائر (المتصفح)، ويسمى هذا الملف "بملف تعريف الارتباط Cookies، وهذا الملف عبارة عن ملفات نصية، تقوم بعض المواقع التي تزورها بإيداعها على القرص الصلب في جهازك، وتحتوي هذه الملفات النصية على معلومات تتيح للموقع الذي أودعها أن يسترجعها عند الحاجة لها خلال زيارة المستخدم المقبلة للموقع ومن هذه المعلومات المحفوظة: - تذكر اسم المستخدم وكلمة المرور.

- حفظ إعدادات الصفحة في حال كان ذلك متاح على البوابة. – عدم إتاحة إمكانية التصويت أكثر من مرة لنفس المستخدم.
- وعلى هذا الأساس فإن بوابة الجامعة ستستخدم المعلومات الموجودة في ملفات تعريف الارتباط لأغراض فنية خاصة بها وذلك عند زيارتها أكثر من مرة، كما أن البوابة بإمكانها تغيير المعلومات الموجودة ضمن ملفات تعريف الارتباط أو إضافة معلومات جديدة كلما قمت بزيارة بوابة جامعة الملك فيصل.
- إذا قمت باستخدام تطبيق مباشر أو أرسلت بريداً إلكترونيًا لإدارة البوابة أو لأي من إدارات الجامعة وذلك عبر البوابة الإلكترونية لجامعة الملك فيصل لكي تزودنا فيه ببيانات شخصية، فإننا قد نشارك هذه البيانات مع جهات أو إدارات أخرى، وذلك لخدمتك بصورة أكثر فعالية. علماً بأننا لن نشارك بياناتك الشخصية مع الجهات غير الحكومية إلا إذا كانت من الجهات المصرح لها ضمن الجهات المختصة بالقيام بأداء خدمات حكومية محددة. وبتقديمك لبياناتك ومعلوماتك الشخصية من خلال البوابة الإلكترونية لجامعة الملك فيصل، فإنك تقر تمامًا بالموافقة على تخزين ومعالجة واستخدام تلك البيانات من قِبل سلطات المملكة العربية السعودية. ونحن نحتفظ بالحق في كل الأوقات في كشف أي معلومات للجهات المختصة، عندما يكون ذلك ضرورياً للالتزام بأي قانون أو نظام أو طلب حكومي.
- إنك مسؤول بمفردك عن تمام وصحة وصدق البيانات التي ترسلها من خلال هذه البوابة.

* فتح حساب في البوابة

- يمكن لمستخدمي البوابة الوصول إلى بعض قواعد المعلومات أو الخدمات التي توفرها البوابة وذلك بعد استلام اسم المستخدم وكلمة المرور التي يتم تحديدها بالتنسيق مع إدارة البوابة. ويمكن أن يُطلب من المستخدم إضافة بعض المعلومات الشخصية أو تحديثها، كما يمكن للمستخدم تعديل أي من بيانات حسابه متى شاء أو حتى إلغائها في أي وقت يرغب في ذلك.
- ومثل أية معلومات أخرى يتم تجميعها حول مستخدمي البوابة، فإن معلومات حساب المستخدم سوف يتم استخدامها لتوثيق شخصية المستخدم وحماية حسابه، كما أنه من الممكن أن تتم مشاركة تلك المعلومات مع أية مواقع أخرى تابعة لبوابة جامعة الملك فيصل.
- يهدف من جمع أي معلومات حول مستخدمي البوابة الأغراض العلمية والبحثية وتطوير خدمات الجامعة بشكل عام والخدمات المقدمة عبر البوابة بشكل خاص وذلك من دوره تعزيز علاقة الجامعة بالمجتمع.

* حماية خصوصية المستخدم

لكي نتمكن من مساعدة المستخدم في حماية معلوماته الشخصية، فإننا نوصي بما يلي:

- الاتصال بنا بشكل فوري عندما يغلب على ظنك أن شخصاً ما استطاع الحصول على كلمة السر الخاصة بك، أو رمز الاستخدام، أو الرقم السري، أو أي معلومات سرية أخرى.
- لا تفصح عن أي معلومات سرية عبر الهاتف أو شبكة الإنترنت ما لم تعرف هوية الشخص أو الطرف المستقبل للمعلومة.
- استخدم متصفحا آمنا عند قيامك بإنجاز المعاملات عبر الإنترنت مع إغلاق التطبيقات غير المستخدمة على الشبكة، والتأكد من أن برنامج الحماية من الفيروسات محدث على الدوام.
- في حالة وجود أية استفسارات أو آراء حول وثيقة الخصوصية وما تحويه من مبادئ، يمكن التواصل مع إدارة البوابة عبر البريد الإلكتروني بالموقع.

للحفاظ على بياناتك الشخصية، يتم تأمين التخزين الإلكتروني والبيانات الشخصية المرسلة باستخدام التقنيات الأمنية المناسبة.

هذه البوابة قد تحتوي على روابط إلكترونية لمواقع أو بوابات قد تستخدم طرقًا لحماية المعلومات وخصوصياتها تختلف عن الطرق المستخدمة لدينا. ونحن غير مسؤولين عن محتويات وطرق وخصوصيات هذه المواقع الأخرى، وننصحك بالرجوع إلى إشعارات الخصوصية الخاصة بتلك المواقع.

* إرسال الرسائل الإلكترونية إلى الجامعة

عندما تقوم بالاستفسار أو طلب معلومات حول معلومة ما أو خدمة محددة أو في حالة قيامك بإعطاء معلومات إضافية مستخدما أياً من وسائل الاتصال مع الجامعة سواء كانت تلك الوسائل إلكترونية أو غير إلكترونية، مثل طلب الاستفسار على موقعنا، فإننا سنستخدم عنوان بريدك الإلكتروني للرد على استفساراتك، ومن الممكن حفظ عنوان بريدك ورسالتك وإجابتنا عليها لأغراض مراقبة الجودة، أو لأجل الغايات القانونية والرقابية.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** قسم النظم والتطبيقات بعمادة تقنية المعلومات بالتنسيق مع إدارة الأمن السيبراني وجميع جهات الجامعة.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢٩. سياسة الاستخدام الآمن للتطبيقات والخدمات الإلكترونية

نطاق العمل وقابلية التطبيق

قامت عمادة تقنية المعلومات بجامعة الملك فيصل بوضع متطلبات سياسة الاستخدام الآمن لتطبيقات الويب، حيث تشمل وتطبق هذه السياسة على كافة منسوبي الجامعة والطلبة وأعضاء هيئة التدريس والمتعاقدين والمقاولين وموظفيهم وعموم المجتمع الذين يستخدمون التطبيقات والخدمات الإلكترونية الخاصة بجامعة الملك فيصل، والهدف من هذه السياسة هو تأمين وحماية الأصول المعلوماتية والموارد والأصول التقنية للجامعة من أي ثغرات أو تهديدات أو اختراقات سيبرانية، كما تعرض السياسة على المستخدم النهائي كيفية استخدامه لهذه الموارد التقنية والمعلوماتية الاستخدام الأمثل للاستفادة من خدمات إلكترونية بمستوى عالٍ من النضج تلبي احتياجات وتوقعات المستفيدين وفق مستويات الحماية المعمول بها وفق سياسات وضوابط وإجراءات الأمن السيبراني الصادرة من الجهات ذات العلاقة في الدولة.

بنود السياسة

يوافق المستخدم النهائي على التقيد التام بهذه السياسة وفي حال عدم الالتزام أو التقيد بها فقد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة. كما يوافق المستخدم النهائي كذلك على عدم استخدام، أو تشجيع، أو تعزيز، أو تسهيل، أو إرشاد الآخرين لاستخدام الأنظمة والتطبيقات والخدمات الإلكترونية، مع الالتزام والتقيد بالتالي:

١. يُمنع على المستخدم الدخول في أنشطة أو الترويج لها أو التشجيع عليها بما يخالف أي قانون، أو نظام، أو قرار حكومي، أو مرسوم ملكي، أو اتفاقية قانونية، أو سياسات.
٢. يُمنع على المستخدم اختراق، أو تعطيل، أو تعديل، أو الدخول، أو الاستخدام، أو الاستغلال غير المشروع للتطبيقات والخدمات الإلكترونية أو قواعد البيانات، أو أنظمة البنية التحتية، وأنظمة الحماية المرتبطة بها سواء على مستوى الشبكة المحلية أو الخارجية.
٣. يُمنع على المستخدم تعطيل أي جانب من جوانب الخدمة أو التدخل فيه أو التحايل عليه؛ أو انتهاك أي إجراءات أمان أو مصادقة يستخدمها النظام أو الخدمة.
٤. يُمنع المستخدم من الدخول على التطبيق أو الخدمة الإلكترونية إذا قام بعدد محدد من محاولات تسجيل الدخول غير الصحيحة مع تعطيل حسابه لفترة زمنية محددة لإحباط أي محاولات للهجوم التخميني.
٥. يُمنع على المستخدم استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية. .
٦. يُمنع على المستخدم الوصول إلى أي خدمة أو نظام أو التحقيق فيه دون تصريح، بما في ذلك، على سبيل المثال لا الحصر، الانتهاكات أو عمليات مسح الثغرات الأمنية أو اختبار الاختراق.
٧. يجب على المستخدم استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.
٨. يجب على المستخدم إبلاغ الجهة المعنية بالأمن السيبراني بالجامعة في حال وجود مواقع مشبوهة ينبغي حجبها أو جدار الحماية Proxy.
٩. يُمنع على المستخدم استخدام التقنيات التي تسمح بتجاوز الوسيط للوصول إلى شبكة الإنترنتFirewall.

١٠. يُمنع على المستخدم أي سرقة للموارد بما في ذلك المعلومات الحساسة.
١١. يُمنع على المستخدم القيام بتزوير أو انتحال هوية الغير أو تغيير هويته وذلك عند استخدام التطبيقات والخدمات الإلكترونية الخاصة بالجامعة.
١٢. يُمنع على المستخدم تنزيل البرمجيات والأدوات أو تثبيتها على أصول الجامعة دون الحصول على تصريح مسبق من عمادة تقنية المعلومات.
١٣. يُمنع على المستخدم استخدام شبكة الإنترنت في غير أغراض العمل بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.
١٤. يجب على المستخدم تبليغ الجهة المعنية بالأمن السيبراني بالجامعة عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.
١٥. يُمنع على المستخدم إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكة الجامعة وأنظمتها أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من الجهة المعنية بالأمن السيبراني بالجامعة.
١٦. يُمنع على المستخدم استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من الجهة المعنية بالأمن السيبراني بالجامعة.
١٧. يُمنع على المستخدم زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.
١٨. يُمنع على المستخدم استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من الجهة المعنية بالأمن السيبراني بالجامعة.
١٩. يُمنع على المستخدم القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من الجهة المعنية بالأمن السيبراني بالجامعة، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.
٢٠. يُمنع على المستخدم تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من عمادة تقنية المعلومات.
٢١. يجب على المستخدم تبليغ الجهة المعنية بالأمن السيبراني بالجامعة عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بجامعة الملك فيصل أو أصولها.
٢٢. يُمنع على المستخدم استخدام البريد الإلكتروني، أو الهاتف، أو الفاكس الإلكتروني، أو وسائل التواصل الأخرى في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني في الجامعة.
٢٣. يُمنع على المستخدم تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.
٢٤. يجب على المستخدم استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.
٢٥. يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بالجامعة في أي موقع ليس له علاقة بالعمل.
٢٦. يجب على المستخدم تبليغ الجهة المعنية بالأمن السيبراني بالجامعة عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة الجامعة أو أصولها.

٢٧. تحتفظ الجامعة بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية والجهة المعنية بالأمن السيبراني بالجامعة وفقاً للإجراءات والتنظيمات ذات العلاقة.

٢٨. يُمنع على المستخدم فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

٢٩. يجب على المستخدم اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة الجامعة وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

٣٠. يُمنع على المستخدم مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو عمادة تقنية المعلومات.

٣١. يجب على المستخدم تغيير كلمة المرور عند تزويده بكلمة مرور جديدة من قبل مسؤول النظام.

٣٢. يجب على المستخدم عدم إفشاء بيانات حسابه الجامعي أو كلمة المرور للآخرين، وتقع المسؤولية على المستخدم نفسه في المحافظة على كافة بياناته الشخصية.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها:** قسم النظم والتطبيقات بعمادة تقنية المعلومات بالتنسيق مع إدارة الأمن السيبراني وجميع جهات الجامعة.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٣٠. سياسة النشر وشروط الاستخدام

نطاق العمل وقابلية التطبيق

أنشأت جامعة الملك فيصل بوابتها الإلكترونية لتكون نافذة فاعلة للتعرف على أنشطة الجامعة وما تقدمه من خدمات للمستفيدين من طلبة الجامعة، أعضاء هيئة التدريس والموظفين، فضلًا عن أي مستفيدين آخرين على المستويين الاقليمي والدولي. وقد حددت إدارة البوابة عدداً من الشروط والبنود التي تشكل فيما بينها سياسة للمستخدم بحيث تحدد العلاقة بين البوابة من جهة، والمستخدمين المستفيدين منها من الجهة الأخرى؛ وهو ما يضمن تقديم خدمة أفضل وبم ا يساعد على تحقيق استفادة أكبر من كل ما تحويه البوابة من معلومات. وبما أن هذه البوابة الإلكترونية لجامعة الملك فيصل بالمملكة العربية السعودية)التي يشار إليها هنا بعبارة "بوابة جامعة الملك فيصل" أو "البوابة"(متاحة لاستخدامك الشخصي؛ فإن دخولك واستخدامك لهذه البوابة يخضع لبنود وشروط الاستخدام، ولأنظمة المملكة العربية السعودية، كما يعد وصولك إلى هذه البوابة ودخولك إليها موافقة دون قيد أو شرط على بنود وشروط الاستخدام سواء أكنت مستخدماً مسجلًا أم لم تكن، وتسري هذه الموافقة اعتباراً من تاريخ أول استخدام لك لهذه البوابة. كما أن من أهم أهداف البوابة، هو أن تكون البوابة واجهة إعلامية معرفية للجامعة وأداة للتيسير على المستفيدين من خدماتها عبر تقديم خدمات إلكترونية فعالة، إلى جانب زيادة الوعي ونشر المعرفة والتأكيد على مبدأ المشاركة والحوار البناء فضلًا عن استعراض دور الجامعة في مسيرة التنمية المستدامة بالمملكة بشكل عام وتطور قطاع التعليم الجامعي ووصوله إلى مراتب متميزة بشكل خاص، وعلى هذا الأساس فإن استخدامك لكل ما يرد بالبوابة إنما يعنى به الاستزادة العلمية والمعرفية والثقافية وهو ما يجعل استخدام أية معلومات ترد بالبوابة على مسؤولية المستخدم الشخصية. ويتضمن استخدام البوابة عدداً من البنود والشروط التي تخضع لتحديثات وتغييرات مستمرة حسب الحاجة، ويصبح أي تعديل أو تحديث لأي من هذه البنود والشروط نافذاً فور اعتماده من إدارة البوابة؛ وهو ما يتطلب منك المراجعة المستمرة لشروط الاستخدام لمعرفة أية تحديثات تتم عليها؛ إذ أن استمرارك في استخدام هذه البوابة يعني اطلاعك وقبولك التام لأي تعديل تم على بنود وشروط الاستخدام. علماً بأن هذه البنود والشروط تتضمن حقوق الملكية، كما أن إدارة البوابة غير مطالبة بالإعلان عن أية تحديثات تتم على تلك الشروط.

بنود السياسة

* قيود الاستخدام:

عند قيام المستخدم النهائي باستخدام البوابة الإلكترونية لجامعة الملك فيصل، فإنه يُقر بالامتناع عما يلي:

- توفير أو تحميل ملفات تحتوي على برمجيات، أو مواد، أو بيانات، أو معلومات أخرى ليست مملوكة لك أو لا تملك لها ترخيصاً.
- استخدام هذه البوابة بأية طريقة لإرسال بريد إلكتروني تجاري أو غير مرغوب فيه أو أية إساءة استخدام لبوابة الجامعة.
- توفير أو تحميل ملفات على هذه البوابة تحتوي على فيروسات أو بيانات تالفة.
- نشر، أو إعلان، أو توزيع، أو تعميم مواد، أو معلومات تحتوي تشويهاً للسمعة، أو انتهاكاً للقوانين، أو مواد إباحية، أو بذيئة، أو مخالفة للتعاليم الإسلامية، أو للآداب العامة، أو أي مواد، أو معلومات غير قانونية من خلال البوابة.

- الاشتراك من خلال البوابة في أنشطة غير مشروعة أو غير قانونية في المملكة العربية السعودية.
- الإعلان على البوابة عن منتج أو خدمة تجعل الجامعة في وضع انتهاك لأي قانون أو نظام مطبق في أي مجال.
- استخدام أية وسيلة، أو برنامج، أو إجراء لاعتراض، أو محاولة اعتراض التشغيل الصحيح للبوابة.
- القيام بأي إجراء يفرض حملًا غير معقول أو كبير أو بصورة غير مناسبة على البنية التحتية لبوابة الجامعة.

* الروابط من وإلى البوابة:

رو ابط من بو ابات جهات أخرى إلى بو ابة الجامعة:

- باستثناء ما هو وارد أدناه، يمنع نقل أو نسخ أي من محتويات البوابة أو إنشاء أية روابط إلكترونية خاصة بها أو عرض أي منها في إطار.
- يمكن وضع روابط خاصة بالبوابة في أية مواقع أخرى لا تتعارض في أهدافها وتوجهها العام مع أهداف وسياسات وأطر عمل البوابة الإلكترونية للجامعة.
- لا تعتبر الجامعة بأي حال من الأحوال مشاركة أو مرتبطة بأي شكل كان بأية علامات، أو شعارات، أو رموز تجارية، أو خدمية، أو أية وسائل أخرى مستخدمة، أو تظهر على مواقع ويب المرتبطة بهذه البوابة أو أي من محتوياتها.
- تحتفظ الجامعة بحقوقها الكاملة في إيقاف وإعاقة أي ارتباط بأي شكل من الأشكال من أي موقع يحتوي على مواضيع غير ملائمة، أو فاضحة، أو متعدية، أو بذيئة، أو إباحية، أو غير لائقة، أو غير مقبولة، أو غير قانونية، أو أسماء، أو مواد، أو معلومات تخالف أي قانون أو تنتهك أية حقوق للملكية الفكرية أو لحقوق الخصوصية أو حقوق العلنية.
- تحتفظ الجامعة بحق تعطيل أي ارتباط بأي شكل من الأشكال غير مصرح به ولا تتحمل أية مسئولية عن المحتويات المتوفرة في أي موقع آخر يتم الوصول إليه عبر هذه البوابة أو الوصول منه لهذه البوابة.

رو ابط من بو ابة الجامعة إلى بو ابات جهات أخرى:

يتم توفير روابط الاتصال الخاصة ببوابات و/أو مواقع ويب أخرى بغرض التسهيل على الزائر، والجامعة وكذا إدارة البوابة غير مسئولين عن محتويات أو مصداقية البوابات و/أو المواقع التي نرتبط بها ولا نصادق على محتوياتها، وبذلك فإن استخدام أي من هذه الروابط للوصول إلى تلك المواقع أو البوابات يتم على مسئوليتك الخاصة بشكل كامل. وإذ نستهدف استبدال الروابط الإلكترونية المقطوعة -التي لا تعمل-بالمواقع الأخرى، وبما إننا لا نملك التحكم أو السيطرة على تلك الروابط؛ فإننا لا نضمن بأي حال أن تعمل هذه الروابط بصورة دائمة.

* الحماية من الفيروسات:

تبذل إدارة البوابة جهداً لفحص واختبار محتويات البوابة الالكترونية لجامعة الملك فيصل في كل مراحل العمل. وننصحك بأن تقوم دائما بتشغيل برنامج مضاد للفيروسات على كل المواد التي يتم تحميلها من الإنترنت. ونحن لا نتحمل أية مسؤولية عن أية خسارة، أو انقطاع، أو تلف لبياناتك، أو جهاز الحاسب لديك والذي قد يحدث أثناء الاتصال بهذه البوابة أو عند استخدام أية مواد من محتوى أو غيره ما يرد فيها.

* التنازل عن المطالبات:

إن البوابة الالكترونية لجامعة الملك فيصل والخدمات المقدمة من خلالها والمعلومات والمواد والوظائف المتاحة عليها أو التي يمكن الوصول إليها من خلال البوابة يتم توفيرها لاستخدامكم الشخصي "كما هي" و "كما هي متاحة" دون أي إقرار أو وعود أو ضمانات من أي نوع. ولا يمكننا أن نضمن أو أن نتحمل المسؤولية عن أية انقطاعات أو أخطاء أو تجاوزات قد تنشأ عن استخدام هذه البوابة أو محتوياتها أو أي موقع يرتبط بها -سواء كان ذلك بعلمنا أو بدون علمنا. إن أية اتصالات أو معلومات قد يقوم المستخدم بإرسالها من خلال هذه البوابة لن يكون له الحق في ملكيتها أو حق ضمان سريتها كما أن أي استخدام عام أو تفاعلي بشكل خاص تتضمنه هذه البوابة لا تضمن أو لا يقصد بها أن تضمن للمستخدم أي حقوق أو تراخيص أو أية امتيازات من أي نوع. وفي حالة تنازلت الجامعة عن أي حق متاح لها ومحدد ضمن هذه الشروط في أحد الأماكن أو إحدى المناسبات، فإن ذلك لا يعني بأي حال تنازلًا تلقائياً وبشكل دائم عن أية حقوق في أماكن ومناسبات أخرى.

* نطاق المسئولية وحدودها:

الخدمات الإلكترونية التي تقدمها البوابة الإلكترونية لجامعة الملك فيصل عبر شبكة الإنترنت والحصول على معلومات بشأن الوكالات، الإدارات، المراكز، الأقسام، الكليات، العمادات، وجميع الجهات المختلفة التابعة للجامعة يتم تقديمها فقط لتسهيل الإجراءات اليدوية. وبهذا تقر بعلمك الكامل بأن الاتصالات عبر شبكة الإنترنت قد تتعرض للتدخل أو الاعتراض بواسطة الغير. وعليه، فان اللجوء إلى هذه البوابة يظل على مسؤوليتك الخاصة، والبوابة لا تتحمل بأي حال من الأحوال المسؤولية عن أية خسارة أو ضرر من أي نوع قد يلحق بك بسبب استخدامك أو زيارتك للبوابة أو اعتمادك على أي بيان أو رأي أو إعلان فيها أو ما قد ينجم عن أي تأخير في التشغيل أو تعثر الاتصال أو مشاكل الدخول إلى شبكة الإنترنت، أو أعطال المعدات، أو البرامج، أو سلوك، أو أفكار أي شخص يدخل إلى هذه البوابة. وبهذا تقر هنا وتوافق على أن وسيلتك الحصرية والوحيدة لعلاج أي ضرر أو خسارة قد تحدث نتيجة دخولك أو استخدامك لهذه البوابة هي الامتناع عن استخدامها أو الدخول إليها أو عدم الاستمرار في ذلك.

* التعويض:

بهذا تقر بعدم اتخاذ أي إجراء ضد جامعة الملك فيصل أو أي من وكالاتها، إداراتها، مراكزها، أقسامها، كلياتها، عماداتها، وجميع الجهات المختلفة التابعة للجامعة؛ وإخلاء المسؤولية عن الجامعة وعن أي الجهات التابعة لها وأي من الموظفين المسؤولين عن إدارة، أو صيانة، أو تحديث، أو تقديم بوابة الجامعة، وذلك فيما يتعلق بكافة الالتزامات والمسئوليات التي قد تطرأ فيما يتصل بأية مطالبات ناشئة عن أي إخلال من جانبك ببنود وشروط الاستخدام، أو أي من القوانين السارية سواء في المملكة العربية السعودية أو المكان الذي تقيم فيه.

* إنهاء الاستخدام:

يجوز لإدارة البوابة وحسب تقديرها المطلق إنهاء أو تقييد أو إيقاف حقك في الدخول إلى البوابة واستخدامها وذلك دون إشعار ولأي سبب بما في ذلك مخالفة شروط وبنود الاستخدام أو أي سلوك آخر قد تعتبره الإدارة حسب تقديرها الخاص غير قانوني أو مضراً بالآخرين، وفي حالة الإنهاء، فإنه لن يكون مصرحاً لك بالدخول إلى هذه البوابة.

* حقوق الملكية:

- تخضع كل مواد المحتوى المنشورة على البوابة وكذلك المواقع التابعة لها لحقوق الملكية الفكرية بما في ذلك النصوص، أو الرسوم، أو الصور، أو البرامج، أو التصاميم وغيرها.
- تسمح إدارة البوابة للمستخدمين باستعراض وتصفح صفحات البوابة والطباعة الورقية وذلك من أجل الاستخدام الشخصي.
- تشرف عمادة تقنية المعلومات فنياً على إدارة البوابة، وهي عمادة تابعة لجامعة الملك فيصل بالمملكة العربية السعودية. وكل المواد المتوفرة في هذه البوابة بما في ذلك النصوص والرسوم التصويرية للمعلومات والبرمجيات (المحتويات) والتصاميم وغيرها محمية بموجب حقوق النشر والعلامات التجارية وأشكال حقوق الملكية الأخرى.
- وبما أن أحد الأهداف الرئيسية للبوابة يتمثل في زيادة الوعي ونشر المعرفة لمستخدمي البوابة وزوارها، فيسمح فقط للمستخدم الشخصي وللاستخدام غير الربحي بالاستفادة من محتوى البوابة وأية معلومات منشورة عليها مع ضرورة الإشارة إلى أن بوابة جامعة الملك فيصل هي مصدر ذلك المحتوى وتلك المعلومات.
- ويمكن في حالة الاستخدام الشخصي طباعة أية أجزاء من المحتوى، وعلى الجانب الآخر فلا يجوز بأي شكل من الأشكال بيع أو ترخيص أو تأجير أو تعديل أو نسخ أو استنساخ أو إعادة طبع أو تحميل أو إعلان أو نقل أو توزيع أو العرض بصورة علنية أو تحرير أو إنشاء أعمال مشتقة من أي مواد أو محتويات من هذه البوابة للجمهور أو لأغراض تجارية، وفي هذه الحالة ولأي استخدام عام لأية أجزاء من محتوى البوابة فيجب الحصول على الموافقة الخطية المسبقة من إدارة البوابة بجامعة الملك فيصل بالمملكة العربية السعودية، مع التأكيد على ضرورة الالتزام بقانون حماية الملكية الفكرية السعودي وكل ما هو منصوص ضمن هذه الوثيقة.
- ويمنع منعا باتا أي تعديل لأي من محتويات البوابة. كما أن الرسومات والصور في هذه البوابة محمية بموجب حقوق النشر، ولا يجوز استنساخها أو استغلالها بأية طريقة كانت دون موافقة خطية مسبقة من إدارة البوابة.
- ينبغي الإشارة المرجعية إلى بوابة جامعة الملك فيصل عند استخدام أي محتوى مذكور على بوابتها الإلكترونية.

* القانون الحاكم والمرجعية القضائية:

بهذا توافق على الخضوع حصريًا للسلطات القضائية بالمملكة العربية السعودية فيما يتعلق بكافة المطالبات والخلافات التي تنشأ عن استخدامك لهذه البوابة، علماً بأن اللغة العربية ستكون هي اللغة الرسمية المستخدمة لحل أية خلافات تنشأ عن استخدامك للبوابة أو أي من محتوياتها.

* شروط عامة:

إن كل المواد والمعلومات المتوفرة على البوابة توعوية وتتعلق بالمجال الأكاديمي وغير هادفة للربح. إن اللغة العربية هي اللغة الأساسية لاستخدام البوابة والاستفادة من كل المواد المنشورة عليها، ويهدف ترجمة أي من هذه المواد لتقديم خدمة مضافة، وعليه فلا يتم الاستناد إلى الترجمة المتوفرة في تفسير أي خلاف حول ما تتضمنه البوابة من محتوى.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني .**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**

- **تنفيذ السياسة وتطبيقها:** قسم النظم والتطبيقات بعمادة تقنية المعلومات بالتنسيق مع إدارة الأمن السيبراني وجميع جهات الجامعة.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٣١. سياسة حسابات التواصل الاجتماعي

نطاق العمل وقابلية التطبيق

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جامعة الملك فيصل بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، وبهدف الوصول إلى فضاء سيبراني آمن وموثوق، وذلك بإعداد ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجامعة، لوضع الحد الأدنى من متطلبات الأمن السيبراني لتمكن الجهات ذات العلاقة بالجامعة من استخدام شبكات التواصل الاجتماعي بطريقة آمنة .

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني .

بنود السياسة

- يجب تقييم مخاطر الأمن السيبراني لحسابات التواصل الاجتماعي، مرة واحدة سنوياً، على الأقل.
- يجب تقييم مخاطر الأمن السيبراني عند التخطيط وقبل السماح باستخدام شبكات التواصل الاجتماعي.
- يجب تضمين مخاطر الأمن السيبراني الخاصة بحسابات التواصل الاجتماعي والخدمات والأنظمة المستخدمة في ذلك في سجل مخاطر الأمن السيبراني الخاص بالجهة، ومتابعته مرة واحدة سنويا، على الأقل.
- يجب عمل توعية بالأمن السيبراني لحسابات التواصل الاجتماعي.
- يجب الاستخدام الآمن لأجهزة المخصصة لحسابات التواصل الاجتماعي والمحافظة عليها.
- يجب تفعيل التعامل الآمن مع هويات الدخول وكلمات المرور والأسئلة الأمنية.
- يجب عدم استخدام حسابات التواصل الاجتماعي الرسمية أغراض شخصية.
- يجب التواصل مباشرة مع بإدارة بالأمن السيبراني في الجامعة حال الاشتباه بتهديد أمن سيبراني .
- استخدام حسابات التواصل الاجتماعي المخصصة للجامعة، وليس الأفراد.
- التسجيل باستخدام معلومات رسمية (بريد الكتروني رسمي خاص لوسائل التواصل الاجتماعي ورقم جوال رسمي)، وعدم استخدام معلومات شخصية.
- استخدام التحقق من الهوية متعدد العناصر **Multi-Factor Authentication** لعمليات الدخول لحسابات التواصل الجامعي.
- تفعيل وتحديث الأسئلة الأمنية وتوثيقها في مكان آمن.
- حصر إمكانية الدخول لحسابات التواصل الجامعي للجهة من أجهزة محددة.

- تطبيق حزم التحديثات، على الأجهزة التي تستخدم في إدارة حسابات التواصل الاجتماعي.
- متابعة حسابات التواصل الاجتماعي ومراقبتها للتأكد من عدم نشر أي محتوى غير مصرح.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني** .
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني**.
- **تنفيذ السياسة وتطبيقها:** كافة جهات ذات العلاقة في الجامعة.

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٣٢. سياسة أمن أجهزة المستخدمين

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن استخدام أجهزة المستخدمين والأجهزة المحمولة (Workstation) داخل جامعة الملك فيصل، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات وسلامتها وتوافرها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضوابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين المكتبية والأجهزة المحمولة داخل جامعة الملك فيصل وتنطبق على جميع منسوبي الجامعة.

بنود السياسة

البنود العامة

١-١ يجب حماية البيانات والمعلومات المُخزّنة في جميع الأنظمة وأجهزة معالجة المعلومات و أجهزة المستخدمين المكتبية والأجهزة المحمولة حسب تصنيفها باستخدام الضوابط الأمنية المناسبة لتقييد الوصول إلى هذه المعلومات، ومنع العاملين غير المصرّح لهم من الوصول لها أو الاطلاع عليها.

٢-١ يجب تحديث برمجيات أجهزة المستخدمين والأجهزة المحمولة، بما في ذلك أنظمة التشغيل والبرامج والتطبيقات، وتزويدها بأحدث حزم التحديثات والإصلاحات وذلك وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في الجامعة (patch management).

٣-١ يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لجميع الأنظمة وأجهزة المستخدمين المكتبية والأجهزة المحمولة وفقاً لمعايير الأمن السيبراني.

٤-١ يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على جميع الأنظمة وأجهزة المستخدمين المكتبية والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.

٥-١ يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.

٦-١ يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع الأنظمة وأجهزة معالجة المعلومات أجهزة المستخدمين والأجهزة المحمولة.

٧-١ يجب السماح فقط بقائمة محددة من التطبيقات (Application Whitelisting) .

١-٨ يجب تشفير وسائط التخزين الخاصة بأجهزة المستخدمين المكتبية والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة وفقا لمعيار التشفير المعتمد في الجامعة .

١-٩ يجب منع وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة الامن السيبراني لامتلاك صلاحية استخدام وسائط التخزين الخارجية .

١-١٠ يجب عدم السماح لأجهزة المستخدمين والأجهزة المحمولة المزودة ببرمجيات غير محدثة أو منتهية الصلاحية (بما في ذلك أنظمة التشغيل والبرامج والتطبيقات) بالاتصال بشبكة الجامعة لمنع التهديدات الأمنية الناشئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.

١-١١ يجب منع أجهزة المستخدمين المكتبية والأجهزة المحمولة غير المزوّدة بأحدث برمجيات الحماية من الاتصال بشبكة الجامعة لتجنب حدوث المخاطر السيبرانية التي تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات. وتتضمّن برمجيات الحماية برامج إلزامية ذات تقنيات وآليات حديثة والمتقدمة وإدارتها بشكل آمن. مثل: برامج الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware)، وجدار الحماية للمستضيف (Host-Based Firewall)

١-١٢ يجب ضبط إعدادات أجهزة المستخدمين للأجهزة المكتبية والأجهزة المحمولة غير المستخدمة بحيث تعرض شاشة توقّف محمية بكلمة مرور في حال عدم استخدام الجهاز (Session Timeout) لأقل مدة ممكنة.

١-١٣ يجب إدارة أجهزة المستخدمين المكتبية والأجهزة المحمولة وأجهزة معالجة المعلومات مركزياً من خلال خادم الدليل النشط (Active Directory) الخاص بنطاق الجامعة أو نظام إداري مركزي.

١-١٤ يجب ربط أجهزة المستخدمين المكتبية والأجهزة المحمولة على الدومين الجامعي KFU Domain وضبط إعدادات أجهزة المستخدمين المكتبية والأجهزة المحمولة بإدارة الوحدات التنظيمية المناسبة (Domain Controller) لتطبيق السياسات الملائمة وتثبيت الإعدادات البرمجية اللازمة.

١-١٥ يجب تنفيذ سياسات النطاق المناسبة (Group Policy) في الجامعة وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة وأجهزة معالجة المعلومات لضمان التزام الجامعة بالضوابط التنظيمية والأمنية.

١- متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

١-٢ يجب تخصيص أجهزة المستخدمين للفريق التقني ذي الصلاحيات الهامة، وأن تكون معزولة في شبكة خاصة لإدارة الأنظمة (Management Network) ولا ترتبط بأي شبكة أو خدمة أخرى.

٢-٢ يجب ضبط إعدادات أجهزة المستخدمين الهامة والحساسة والتي لها صلاحيات متقدمة لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني، مع عدم إمكانية إيقافه عن طريق المستخدم.

٣-٢ يجب تأمين أجهزة المستخدمين مادياً داخل مباني الجامعة.

٤-٢ التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية والامن المتعلق بها .

٢- متطلبات أخرى

٥-١ يجب نشر الوعي الأمني للعاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول المعتمدة في الجامعة وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصلاحيات الهامة والحساسة.

٥-٢ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والأجهزة المحمولة.

٥-٣ يمنع اتصال الأجهزة المحمولة الشخصية (الغير مرتبطة بالمجال الجامعي) بشبكة الجامعة الداخلية .

٥-٤ يقتصر ربط الأجهزة الشخصية المحمولة بشبكة الضيوف الآمنة و المعزولة KFU Guest.

٥-٥ يمنع حفظ البيانات الخاصة بالجامعة على الأجهزة المحمولة والشخصية.

٥-٦ يجب مراجعة سياسة أمن أجهزة المستخدمين المكتبية والأجهزة المحمولة وأجهزة وأنظمة معالجة المعلومات سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني**
- **مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.**
- **تنفيذ السياسة وتطبيقها: إدارة الأمن السيبراني.**

الالتزام بالسياسة

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق وتنفيذ سياسات الأمن السيبراني ومعاييره.
- يجب على جميع منسوبي الجامعة الالتزام بهذه السياسة.
- قد يُعرّض أي انتهاك لهذه السياسة والسياسات ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

القسم الثالث

مجموعة المعايير التقنية

للأمن السيبراني

ا. معيار أمن الشبكات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية أمن الشبكات الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية، وهي: سرية المعلومات، وسلامتها، وتوافرها.

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أنظمة الشبكات التقنية الخاصة بجامعة الملك فيصل، وينطبق على جميع منسوبي جامعة الملك فيصل.

المعايير

ا-١ الوصول الآمن (Secure Access)

الهدف

ضمان تطبيق الإعدادات الصحيحة للوصول إلى واجهات إدارة أمن الشبكات من أجل حمايتها بشكل فعال من الهجمات السيبرانية.

المخاطر المحتملة

تؤدي الإعدادات غير الكافية لحلول واجهات إدارة أمن الشبكات إلى تعرض أجهزة الشبكات داخل بيئة جامعة الملك فيصل إلى هجمات أو انتهاكات أمنية يصعب اكتشافها.

الإجراءات المطلوبة

١- إعداد قوائم الوصول بصورة تسمح بالتحكم بالوصول إلى أجهزة اتصالات الشبكة بحيث يمكن للأشخاص المصرح لهم فقط الوصول إلى هذه الأجهزة.

٢- إعداد قائمة وصول لحماية جميع أجزاء الشبكة من انتحال عنوان بروتوكول الإنترنت (IP Address Spoofing).

٣- استخدام آلية تحقق مركزية للتحقق من جميع المستخدمين التفاعليين الذين يقومون بعمل تغييرات على كافة أجهزة الشبكة. كما يجب أن تكون أنظمة التحقق بأقل عدد ممكن.

٤- استخدام المشرفين لأجهزة حاسب ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs) أو خوادم الوصول إلى المناطق الآمنة (Jump Servers) الموجودة على واجهات إدارة مستقلة على شبكة مفصولة عن شبكة الجامعة ومعزولة عن الإنترنت.

٥- تطبيق التحقّق من الهوية متعدّد العناصر واستخدام الجلسات المشفرة لإدارة كافة أجهزة الشبكات.

٦- تقييد استخدام كلمة المرور المحددة بتعليمات ثابتة وحصره على مشرفين محددين فقط بحسب ما هو ضروري لغايات غير تفاعلية ولاستعادة أجهزة الشبكة التي تم فصلها عن الشبكة.

٧- إعداد أجهزة الشبكة لعرض رسالة نصية تنبيهية عند تسجيل الدخول. ويجب ألا تُظهر هذه الرسالة النصية الخصائص الأساسية للشبكة.

٢-١ فصل الشبكة (Network Segregation)

الهدف

ضمان حماية تصميم وبنية الشبكة وحماية الأجزاء الشبكية وفقاً لمستوى الأمن الخاص بها.

المخاطر المحتملة

تتشارك الشبكات غير المفصولة في نفس نطاق البث وتكون الأجهزة قادرة على التواصل دون مراقبة أو ضبط حركة البيانات، وبالتالي يمكن أن يؤدي أي هجوم على النظام إلى تهديدات داخلية خطيرة وهجمات على معظم أنظمة الشبكة، مما يسهل حركة البيانات الجانبية ضمن الشبكة.

الإجراءات المطلوبة

١- تصميم وتطبيق شبكة معزولة منطقياً و/أو مادياً مع الأخذ بعين الاعتبار احتياجات الأعمال والمعمارية المؤسسية وذلك بالاستناد إلى الدفاع الأمني متعدد المراحل والمعمارية متعددة المستويات.

٢- تطبيق المستوى الملائم من ضوابط الأمن السيبراني على الأجزاء الشبكية المختلفة بناءً على قيمة وتصنيف المعلومات المخزنة أو المعالجة في الشبكة ومستويات الموثوقية والتأثير على الأعمال والمخاطر المرافقة.

٣- تطبيق المعمارية متعددة المستويات المحمية بجدار حماية ثنائي الطبقة. وعلى وجه الخصوص، تقسيم الشبكة إلى ثلاثة مستويات أو أكثر (مستوى الحدود/المحيط، والمستوى الرئيسي، والمستوى الموثوق)، وتقسيم الأجزاء الشبكية إلى مناطق (المنطقة المحايدة "DMZ"، ومنطقة الإدارة، ومنطقة الإنتاج، ومنطقة التطوير/الاختبار، وغيرها) وفقاً للبنية المؤسسية والبنية الأمنية في جامعة الملك فيصل.

٤- تصميم وإعداد الشبكات لتصفية مرور البيانات بين مختلف الأجزاء وحجب الوصول غير المصرح به.

٥- وضع الخوادم أو مخازن البيانات التي تتضمن معلومات محمية في أجزاء شبكية منفصلة ومخصصة.

٦- إعداد جدران الحماية والموجّهات (Routers) لمنع أي اتصالات غير مصرح بها بين الشبكات غير الموثوقة وأي مكونات نظام تقوم بتخزين معلومات حساسة أو حساسة جداً.

٧- تحديد وتطبيق المستويات والحدود لكل منطقة أمنية.

٨- تحديد وتطبيق منطقة أو جزء شبكي لواجهات الإدارة المستقلة، بما في ذلك كافة خوادم الإدارة، والمعدات ذات صلاحية الوصول الإدارية، وخوادم بروتوكول النقل الآمن (SSH)، وخوادم الوصول إلى المناطق الآمنة (Jump Servers)، وأجهزة الحاسب ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs).

٩- فصل الشبكات اللاسلكية عن الشبكة الداخلية والشبكات المعزولة والشبكات الخاصة.

١٠- تحديد الخوادم والشبكات وبيئات الإنتاج والاختبار والبيئات الموثوقة المستخدمة في تطوير واختبار وفحص وتخزين البيانات والنشاطات ذات الصلة بوضوح وفصلها عن الشبكات الأخرى.

١١- فصل أجزاء الأنظمة الحساسة منطقياً عن البيئات الأخرى.

١٢- منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية.

١٣- منع الأنظمة الحساسة من الاتصال بالإنترنت في حال كانت هذه الأنظمة تقدم خدمات داخلية لا تحتاج إلى صلاحية الوصول عن بعد أو الوصول عبر الإنترنت.

١٤- مراجعة الإعدادات والقواعد والسياسات والملفات التعريفية الأمنية لجدران الحماية والموجهات (Routers) التي تدعم الشبكات الحساسة مرة كل ستة أشهر على الأقل.

٣-١ تأمين الحدود (Boundary Defense)

الهدف

حماية حدود الشبكة من التهديدات.

المخاطر المحتملة

في حال تم ترك حدود الشبكة من دون الحماية التي توفرها الضوابط الأمنية المناسبة، سيتمكن المهاجمون من اختراق الشبكة بسهولة وفرض المزيد من التهديدات الخطيرة.

الإجراءات المطلوبة

١- الاحتفاظ بقائمة جرد محدثة لكافة حدود الشبكة في جامعة الملك فيصل.

٢- القيام بعمليات مسح وفحص منتظمة من الخارج لكل حد شبكة موثوق لاكتشاف أي اتصالات غير مصرح بها يمكن الوصول إليها عبر الحدود.

٣- حظر الاتصالات مع عناوين بروتوكولات الإنترنت الخبيثة أو غير المستخدمة وحصر الوصول بمجالات عنوان بروتوكولات الإنترنت الموثوقة والضرورية عند كل حد من حدود شبكة الجامعة.

٤- حظر الاتصالات عبر منافذ بروتوكول التحكم بالنقل (TCP) أو بروتوكول حزم بيانات المستخدم (UDP) أو حركة التطبيقات لضمان السماح فقط للبروتوكولات المصرح لها بالدخول أو الخروج من الشبكة عبر حدود الشبكة عند كل حد من حدود شبكة الجامعة.

٥- إعداد أنظمة المراقبة لتسجيل حزم بيانات الشبكة التي تمر عبر الحدود عند كل حد من حدود شبكة الجامعة.

٦- تثبيت حساسات أنظمة كشف التسلل (IDS) على الشبكة لكشف أي آليات هجوم غير اعتيادية وكشف أي انتهاكات أمنية لهذه الأنظمة عند كل حد من حدود شبكة الجامعة.

٧- تثبيت أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات على الشبكة لكشف أي حركة بيانات خبيثة على الشبكة عند كل حد من حدود شبكة الجامعة.

٨- تثبيت تقنيات كشف/منع التهديدات المتقدمة المستمرة (APT) على الشبكة لكشف أو حجب الهجمات على الشبكة والهجمات غير المعروفة مسبقاً عند كل حد من حدود شبكة الجامعة.

٩- تثبيت جدار حماية التحقق من التطبيقات لحجب أي تطبيقات غير مدرجة في قائمة التطبيقات المسموحة أو غير معروفة أو لا تمتثل للضوابط الأمنية (مثل التطبيقات التي تتواصل عبر منفذ بروتوكول حزم بيانات المستخدم الخاص بنظام أسماء النطاقات "UDP/53" وهي غير ممتثلة لبروتوكول نظام أسماء النطاقات) عند كل حد من حدود شبكة الجامعة.

١٠- تثبيت جدار الحماية لتطبيقات الويب (WAF) لتحليل وتصفية ومراقبة حركة البيانات، ومنع حركة بيانات غير المصرح لها من وإلى تطبيقات الويب.

١١- ضبط إعدادات بروتوكولات التشفير المقبولة والموافق عليها مثل بعض أنواع أمن طبقة النقل (TLS) للعمل على أي جهاز من أجهزة جدران الحماية لتطبيقات الويب (WAF) للتحقق من البيانات غير المشفرة. وفي حال عدم دعم الجهاز عملية تفريغ البيانات عبر أمن طبقة النقل، فلا بد من وضع جدار الحماية لتطبيقات الويب في جهاز فك تشفير للتحقق من البيانات غير المشفرة، أو تثبيت جدار الحماية لتطبيقات الويب على المستضيف.

١٢- تمكين جمع معلومات حركة البيانات عبر الشبكة (NetFlow) وتسجيل البيانات على كافة أجهزة حدود الشبكة.

١٣- ضمان أن كافة أشكال حركة البيانات عبر الشبكة من أو إلى الإنترنت تمر عبر خادم وكيل طبقة التطبيقات المعتمدة والمجهز لتصفية الاتصالات غير المصرح بها.

١٤- السماح للمستخدمين بالوصول إلى فئات عناوين (URL) محددة ومصرح بها، وحجب إمكانية الوصول إلى فئات العناوين (URL) الضارة أو المخصصة للاختراق، أو التي تعمل عبر خوادم مفوضة أو خوادم غير معروفة الهوية، أو المخصصة للتصيّد، أو المشبوهة، أو غير المعروفة، أو غير المصنفة.

١٥- فك تشفير كافة حركة بيانات تصفح الإنترنت المشفرة عند الخادم المفوض على الحدود قبل تحليل المحتوى. يمكن لجامعة الملك فيصل استخدام قائمة محددة من التطبيقات لمواقع مسموحة يمكن الوصول إليها عبر خادم وكيل دون فك تشفير حركة البيانات.

١٦- ضبط إعدادات الوصول وتسجيل الدخول عن بعد إلى شبكة الجامعة للقيام بتشفير البيانات قيد الاستخدام والنقل، واستخدام التحقّق من الهوية متعدّد العناصر.

١٧- تثبيت جهاز وصول عن بعد يستخدم تقنيات مثل الشبكات الخاصة الافتراضية أو حلول طبقة المنافذ الآمنة-الشبكات الخاصة الافتراضية (SSL-VPN) لحجب وحماية كافة أشكال الوصول إلى شبكة الجامعة.

١٨- مسح جميع أجهزة المشاريع التي تقوم بالدخول عن بعد إلى شبكة الجامعة قبل وصولها إلى الشبكة لضمان تطبيق جميع سياسات الأمن المعتمدة في جامعة الملك فيصل بنفس الطريقة التي تم تطبيقها على أجهزة الشبكة المحلية.

١٩- تثبيت تقنيات كشف/منع هجمات حجب الخدمة (DoS) وهجمات تعطيل الخدمات الموزعة (DDoS) على أجهزة جامعة الملك فيصل أو من قبل أطراف خارجية لكشف وحجب هجمات حجب الخدمة (DoS) عند كل حد من حدود شبكة الجامعة.

٢٠- تثبيت تقنيات أمن نظام أسماء النطاقات لكشف أو حجب الهجمات على نظام أسماء النطاقات عند كل حد من حدود شبكة الجامعة.

٢١- تمكين تسجيل الاستفسارات على نظام أسماء النطاقات لكشف وتحديد اسم المستضيف للنطاقات الخبيثة المعروفة.

٢٢- تثبيت بوابة أمن البريد الإلكتروني لكشف أو حجب الهجمات عبر البريد الإلكتروني على حدود شبكة الجامعة.

٢٣- ضمان التحديث المنتظم لكافة خدمات الاشتراك وفئات العناوين (URL) ومصادر المعلومات الاستباقية والقوائم المحددة من التطبيقات الممنوعة (Blacklists) والإشارات المعرفة المسبقة.

١-٤ القيود والضوابط (Limitations and Controls)

الهدف

الحد من مصادر الهجمات وحماية الشبكة الداخلية من التهديدات.

المخاطر المحتملة

تؤدي حماية الشبكة الداخلية إلى تقليل مخاطر التهديدات الداخلية والحركة الجانبية (Network Lateral Movement).

الإجراءات المطلوبة

١- ربط المنافذ والخدمات والأجهزة النشطة بأصول المعدات في قائمة جرد الأصول.

٢- تقييد منافذ الشبكة وبروتوكولاتها والخدمات المتاحة على النظام وحصرها على متطلبات الأعمال لكل نظام.

٣- القيام بعمليات مسح آلية للمنافذ بشكل منتظم على كافة الأنظمة، والتنبيه عند اكتشاف منافذ غير مصرح بها على النظام.

٤- تطبيق جدار حماية المستضيف أو أدوات تصفية المنافذ لكل نظام مع تطبيق قاعدة المنع التلقائي التي تحجب جميع أشكال حركة البيانات باستثناء الخدمات والمنافذ المصرح لها فقط.

٥- تثبيت جدار حماية لمركز البيانات لفحص ومراقبة الاتصالات عبر الشبكة المحلية الافتراضية (VLAN)، والمنافذ الموثوقة وغير الموثوقة، وما بين المناطق والأجزاء والخوادم لحماية الشبكات الداخلية وحجب الهجمات الداخلية.

٦- إعداد سياسات جدار الحماية ونموذج القواعد لاتباع نموذج الأمن الإيجابي (نموذج السماح بقائمة محددة من التطبيقات) من خلال حجب كافة أنواع حركة البيانات تلقائياً والسماح فقط بحركة بيانات محددة إلى خدمات معينة. ويمكن تحقيق هذا الأمر من خلال ضبط إعدادات آخر قاعدة في قائمة التحكم بالوصول بحيث تحجب كافة أنواع حركة البيانات. ويمكن القيام بهذا الأمر بشكل صريح أو ضمني حسب المنصة.

٧- إعداد جدار حماية لمركز البيانات مجهز بآلية التعرف على التطبيقات (المستوى ٤- المستوى ٧) وآلية السماح بقائمة محددة من التطبيقات (Whitelisting) ومنع قائمة محددة أخرى من التطبيقات (Blacklisting).

٨- ضبط إعدادات قوائم جدار الحماية بآلية التعرف على المستخدم لوضع السياسات بناءً على هوية المستخدم (UID).

٩- في حال كانت شبكة الجامعة تعمل على الإصدار الرابع من بروتوكول الإنترنت (IPv4)، يجب تثبيت ضوابط الأمن من المستوى ٢ لحماية الشبكة الداخلية.

١٠- تطبيق كافة الضوابط المذكورة أعلاه في هذا المعيار على الشبكة الداخلية للجامعة.

١١- إعداد شبكات محلية افتراضية خاصة/معزولة لأجزاء الشبكة الحساسة أو الأجزاء المعزولة.

١٢- منع إمكانية وصول الشبكات أو أجزاء الأنظمة الحساسة إلى أي نظام في البيئة ما لم يتم مسحها مع تطبيق الضوابط الأمنية المطلوبة والتحقق من الوضع الأمني للنظام.

١٣- عزل شبكة الاتصالات من خلال وضعها في شبكات محلية افتراضية منفصلة وملائمة بناءً على وظيفتها مع استغلال الشبكات المحلية الافتراضية الخاصة أو التجزئة الدقيقة للشبكة.

٥-١ الوصول اللاسلكي (Wireless Access)

الهدف

ضبط استخدام الشبكات اللاسلكية وحمايتها.

المخاطر المحتملة

في حال تم ترك الشبكات اللاسلكية من دون حماية، ستتعرض جامعة الملك فيصل لمخاطر الاتصال غير المصرح به بالشبكة أو كشف البيانات.

الإجراءات المطلوبة

١- إجراء تقييم مخاطر شامل لتقييم مخاطر اتصال الشبكات اللاسلكية بالشبكة الداخلية.

٢- الاحتفاظ بقائمة جرد بنقاط الوصول اللاسلكية المصرح بها والمتصلة بالشبكة السلكية.

٣- إعداد أدوات مسح الثغرات الأمنية في الشبكة لكشف أو منع أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده.

٤- استخدام نظام كشف التسلل اللاسلكي (WIDS) لكشف أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده.

٥- إلغاء تفعيل الوصول اللاسلكي على الأجهزة التي لا تقتضي طبيعة عملها ذلك.

٦- إعداد الوصول اللاسلكي على أجهزة المتصلين التي لا تحتاج لذلك لغايات العمل بحيث يتم السماح بالوصول إلى الشبكات اللاسلكية المصرح بها فقط وتقييد الوصول إلى الشبكات اللاسلكية الأخرى.

٧- إلغاء تفعيل قدرات الشبكة اللاسلكية (المخصصة) لمشاركة الملفات بين الأجهزة مباشرة على الشبكات اللاسلكية لدى المتصلين.

٨- إعداد نقاط الوصول اللاسلكية والأجهزة اللاسلكية للاتصال بالشبكة اللاسلكية باستخدام بروتوكولات آمنه مثل (WPA2) أو (WPA3).

٩- ضمان استخدام الشبكات اللاسلكية لبروتوكولات التحقق مثل بروتوكول المصادقة القابل للامتداد-أمن طبقة النقل (EAP/TLS) الذي يقتضي استخدام التحقّق من الهوية متعدّد العناصر بشكل متبادل.

١٠- إلغاء تفعيل الوصول اللاسلكي للأجهزة الطرفية الموجودة على الأجهزة (مثل تقنية بلوتوث "Bluetooth" والاتصال قريب المدى "NFC") ما لم تقتض طبيعة العمل ذلك.

١١- إيجاد شبكات لاسلكية منفصلة للأجهزة الشخصية أو غير الموثوقة، والتعامل مع هذه الشبكات بحذر واعتبارها مصادراً غير موثوقة مما يستدعي مراقبتها وتصفيتها بشكل مستمر.

٦-١ التشفير (Cryptography)

الهدف

ضمان الحفاظ على سريّة حركة بيانات الشبكة والتأكّد من سريتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات المحمية.

المخاطر المحتملة

قد يؤدي عدم وجود التقنيات الأمنية المناسبة لضمان تشفير بيانات الشبكة إلى تعرض بيانات جامعة الملك فيصل لمخاطر سيبرانية عالية نتيجة الوصول غير المصرح به إليها.

الإجراءات المطلوبة

١- وضع ضوابط على استخدام بروتوكولات الإدارة المشفرة الآمنة، مثل بروتوكول النقل الآمن (SSHv2) وبروتوكول التحكم بسطح المكتب عن بعد (RDP) عبر أمن طبقة النقل (TLS).

٢- تشفير حركة بيانات الشبكة السرية والمحمية باستخدام الجيل التالي من خوارزميات التشفير المدعومة (مثل التشفير بمجموعة "Suite B"). يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة الملك فيصل.

٣- تشفير حركة بيانات الوصول عن بعد عبر أمن بروتوكول الإنترنت (IPSec) أو أمن طبقة النقل (TLS) باستخدام الجيل التالي من خوارزميات التشفير المدعومة (مثل التشفير بمجموعة "Suite B"). يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة الملك فيصل.

٤- إعداد بروتوكولات التطبيقات لتستخدم التشفير حيثما أمكن (مثل: بروتوكول نقل النص التشعبي الآمن "HTTPS" وبروتوكول النقل الآمن "FTPS" عبر طبقة المنافذ الآمنة "SSL"، وبروتوكول النفاذ إلى الدليل البسيط "LDAP" عبر طبقة المنافذ الآمنة "SSL").

V-I الأمن المادي (Physical Security)

الهدف

ضمان حماية جميع أجهزة الشبكة المطلوبة لاتصالات الشبكة من العبث أو التعديل أو أي هجمات مادية أخرى.

المخاطر المحتملة

يمكن أن يؤدي الهجوم المادي على أجهزة الشبكة التي تحفظ عمليات الاتصالات إلى الإضرار بالأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل، وبالتالي التأثير على سير أعمالها المعتاد. في حال تلف الجهاز أو العبث به أو تعديله مادياً، لا يمكن لجامعة الملك فيصل الوثوق بالمعلومات المرسلة عبره وسيرتفع مستوى المخاطر التي قد تهدد أمن الشبكة.

الإجراءات المطلوبة

١- وضع كافة أجهزة الشبكة المطلوبة لاتصالات الشبكة في منطقة آمنة مع تطبيق ضوابط الوصول المادي عليها.

٢- وضع معدات الشبكة الرئيسية في منطقة محمية بنظام إنذار.

٣- ربط معدات الشبكة الرئيسية بمولد طاقة غير منقطعة (UPS) أو نظام توليد للطاقة.

٤- إعداد آليات الدفاع المادية في أجهزة الشبكة، بما في ذلك آليات مثل:

- الحماية عبر إعدادات نظام الإدخال/الإخراج الأساسي (BIOS).
- نظام الإنذار بوجود محاولة لفتح هياكل الأجهزة.

٥- تمكين تلك الآليات في حال توفرها للتقنيات الموجودة.

٨-١ التسجيل والمراقبة (Logging and Monitoring)

الهدف

ضمان مراقبة وتخزين كافة الأحداث الحساسة المتعلقة بأمن الشبكة من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال جامعة الملك فيصل.

المخاطر المحتملة

لضمان سلامة الشبكة، يجب مراقبة كافة أجهزة الشبكة بشكل منتظم وضمان إمكانية الوصول إليها من قبل فرق الأمن السيبراني في جامعة الملك فيصل. دون القدرة على مراقبة وتسجيل الأحداث في الشبكة، لن تتمكن جامعة الملك فيصل من التحقيق في الهجمات التي يتعرض لها أمن الشبكة مما يؤدي إلى زيادة تكرار تلك الهجمات.

الإجراءات المطلوبة

١- إعداد كافة أجهزة الأمن والشبكة لتسجيل سجلات الأحداث والتدقيق في نظام إدارة الأحداث والسجلات المركزي لأغراض التحليل والربط والتنبيه وفقاً لمعيار إدارة ومراقبة سجل الأحداث المعتمد في جامعة الملك فيصل.

٢- ضمان اتساق كافة سجلات الأجهزة مع متطلبات معيار إدارة ومراقبة سجل الأحداث المعتمد في جامعة الملك فيصل.

٣- إعداد جميع أجهزة أمن الشبكة لتسجيل كافة طلبات شريط العنوان (URL) وكافة الجلسات المحجوبة وأحداث التهديدات.

٤- إعداد أجهزة الشبكة لإرسال الأحداث المتعلقة بمحاولات الدخول الناجحة وغير الناجحة إلى واجهات الإدارة إلى نظام إدارة الأحداث والسجلات المركزي لأغراض التحليل والربط والتنبيه.

٥- تخزين كافة السجلات في بيئة آمنة مع تفعيل خاصية التحكم بالوصول إليها.

٩-١ الإعدادات والتحصين والنسخ الاحتياطية (Secure Configuration and Backup)

الهدف

ضمان أن عملية الرقابة على التغييرات يتم تطبيقها على المخاطر التقنية والأمنية بشبكة الجامعة.

المخاطر المحتملة

لضمان سلامة الشبكة، يجب عمل نسخ احتياطية من الإعدادات قبل تنفيذ أي تغييرات قد تعرض شبكة الجامعة إلى مخاطر كبيرة، كما يجب وضع سجل بالتغييرات لتتبعها وتحديد الجهات المسؤولة عنها.

الإجراءات المطلوبة

١- صياغة الحد الأدنى من المعايير الأمنية الأساسية (MBSS) لكافة أجهزة الشبكة.

٢- مراجعة الحد الأدنى من المعايير الأمنية الأساسية (MBSS) بشكل منتظم لكافة الأجهزة مرة واحدة كل ٦ أشهر على الأقل.

٣- ضمان امتثال جميع الأجهزة بالحد الأدنى من المعايير الأمنية الأساسية (MBSS) والإبلاغ عن أي انحرافات يتم اكتشافها.

٤- تطبيق واتباع عملية الرقابة على التغيير لأي تغييرات تنطوي على مخاطر كبيرة على شبكة الجامعة، بما في ذلك القواعد المنطقية Logical Rules التي تسمح بتدفق حركة البيانات عبر أجهزة الشبكة وسياسات أمن جدران الحماية وترجمة عنوان الشبكة (NAT)، وغيرها. ويجب توثيق هذه العملية بما في ذلك العناصر التالية:

- الغاية من القاعدة المنطقية Logical Rule
- الخدمات أو التطبيقات المتأثرة
- المستخدمون والأجهزة المتأثرة
- تاريخ إضافة القاعدة المنطقية Logical Rule
- تاريخ انتهاء صلاحية القاعدة المنطقية Logical Rule، إذا كان ينطبق ذلك
- اسم الشخص الذي أضاف القاعدة المنطقية Logical Rule
- بيان المشكلة
- البيانات الداعمة
- موافقة الإدارة على التغييرات

٥- عمل نسخ احتياطية من الإعدادات لكافة معدات الشبكة المتضررة من التغيير قبل تطبيق التغيير على أرض الواقع.

٦- إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في جامعة الملك فيصل.

٧- إجراء التحديثات والإصلاحات على أجهزة الشبكات بشكل منتظم وفقاً لسياسة إدارة التحديثات والإصلاحات في جامعة الملك فيصل لضمان تحديث جميع البرامج الثابتة على الأجهزة وتطبيق التحديثات والإصلاحات.

٨- إزالة/إلغاء تفعيل الخدمات غير الضرورية أو غير اللازمة على أجهزة الشبكة مثل: بروتوكول النقل الآمن (FTP) أو بروتوكول تل نت (Telnet) أو غيرها.

٩- إعداد وضبط كافة أجهزة الشبكة ليتزامن وقتها مع ثلاث خوادم زمنية إضافية على الأقل.

١٠-١ التحقق من سلامة البرمجيات والمعدات (Hardware and Software Integrity Validation)

الهدف

ضمان أن جميع برامج ومعدات الشبكة تأتي من الجهة المصنعة للمعدات أو المالكة للبرمجيات وأنه لم يتم العبث بها والتحقق من ذلك من خلال التدقيق الدوري.

المخاطر المحتملة

تعتبر الاختراقات في سلسلة الإمداد فرصة لتركيب وتثبيت البرامج والمعدات الخبيثة ضمن شبكة الجامعة، وقد تؤثر البرامج والمعدات التي تتعرض لانتهاك أمني على أداء الشبكة وتهدد سرية وسلامة وتوافر المعلومات الخاصة بجامعة الملك فيصل. ونتيجة لذلك، سيصبح من الممكن تحميل البرمجيات غير المصرح بها أو الخبيثة على الجهاز بعد تشغيلها.

الإجراءات المطلوبة

١- فحص كافة أجهزة الشبكة المادية بحثاً عن أي علامات لوجود عبث عند التركيب.

٢- الحصول على البرمجيات وتحديثات النظام وحزم التحديثات والإصلاحات والترقيات الخاصة بمكونات الشبكة من مصادر موثوقة.

٣- أثناء تنزيل البرمجيات من الإنترنت، يجب التحقق من التجزئة مع قاعدة بيانات المورد لكشف أي تعديل غير مصرح به على البرامج الثابتة أو البرمجيات.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٢. معيار حماية البريد الإلكتروني

الأهداف

يهدف هذا المعيار إلى توفير متطلبات الأمن السيبراني التقنية المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن استخدام جامعة الملك فيصل للبريد الإلكتروني وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي:

- سرية معلومات البريد الإلكتروني.
- سلامة معلومات البريد الإلكتروني.
- توافر خدمة البريد الإلكتروني.

يتبع هذا المعيار المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهو متطلب تشريعي في الضابط رقم ١-٣-٣ والضابط رقم ٢-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أنظمة البريد الإلكتروني الخاصة بجامعة الملك فيصل، وينطبق على جميع مستخدمي البريد الإلكتروني في جامعة الملك فيصل.

المعايير

٢-١ تصفية المحتوى وتحليله (Content Filtering and Analysis)

الهدف

ضمان حماية عناوين البريد الإلكتروني من الرسائل الاقتحامية (Spam Emails) والتصيّد الإلكتروني (Phishing Emails) وروابط الإنترنت الضارة والمشبوهة (Malicious URLs) وأي نوع آخر من المحتوى الضار.

المخاطر المحتملة

يُمكن أن ينخدع المستخدم برسائل البريد الإلكتروني التي تحتوي على محتوى ضار ومشبوه، وقد تتعرّض جامعة الملك فيصل لهجمات سيبرانية في حال عدم فحص رسائل البريد الإلكتروني والتأكد من سلامتها.

الإجراءات المطلوبة

١- فحص جميع رسائل البريد الإلكتروني الواردة والصادرة الخاصة بجامعة الملك فيصل من المحتوى الضار والمشبوه (Malicious Content).

٢- ترميز أو وضع علامة (Tag/Label) على جميع رسائل البريد الإلكتروني الواردة والصادرة الخاصة بجامعة الملك فيصل بالترميزات الوقائية المناسبة بما يعكس مستوى الحساسية والسريّة بناءً على مستوى تصنيف البيانات ووفقاً لنتيجة تحليل المحتوى، أو

استخدام إجراء الترميز المعياري (Tagging/Labeling Standard) المطبّق في جامعة الملك فيصل وفقاً لسياسة أمن البريد الإلكتروني المتّبعة فيها. من الأمثلة على الترميزات أو العلامات: محتوى ضار، ومُرسِل غير مصرّح له، وغير لائق، ورسالة اقتحامية، ورسالة اقتحامية مشتبهة (Suspected SPAM)، وآمن، وحسّاس، وغيرها.

٣- حجب جميع رسائل البريد الإلكتروني الواردة بترميزات أو علامات وقائية تُشير إلى المحتوى غير المسموح به وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في جامعة الملك فيصل، على سبيل المثال:

- حجب الرسائل الخبيثة وغير المصرّح بها والاقتحامية.
- حجر الرسائل الاقتحامية المشتبهة.
- السماح بالرسائل الآمنة.

٤- حجب جميع رسائل البريد الإلكتروني الصادرة والمصنفة، بناءً على ترميزات أو علامات وقائية تُشير إلى مستوى سريّة رسالة البريد الإلكتروني وذلك وفقاً لسياسة أمن البريد الإلكتروني المتّبعة وسياسة تصنيف البيانات في جامعة الملك فيصل، على سبيل المثال:

- حجب الرسائل الحسّاسة والسريّة.
- السماح بالرسائل العامة والخاصة.

٥- حجب رسائل البريد الإلكتروني الاقتحامية التي تتضمّن درجات غير مسموح بها من المخاطر الاقتحامية وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في جامعة الملك فيصل، على سبيل المثال:

- حجب الرسائل شديدة المخاطر.
- حجر الرسائل متوسطة المخاطر.
- السماح بالرسائل منخفضة ومعدومة المخاطر.

٦- حجب رسائل البريد الإلكتروني الواردة التي تحتوي على روابط إنترنت ونطاقات ضارة ومشبوهة (Malicious URLs and Domains) ومحاولات تصيّد وما إلى ذلك.

٧- استبدال عناوين الويب النشطة (Active Web Addresses) المُدرجة في نص رسالة البريد الإلكتروني بعناوين أخرى.

٨- حجب رسائل البريد الإلكتروني الواردة التي تحتوي على محتوى تفاعلي (Active Content) في نص الرسالة الإلكترونية أو حذفه منها.

٩- حجب رسائل البريد الإلكتروني الواردة والصادرة التي تحتوي على ملفات أو محتويات حجمها أكبر من الحجم المسموح حسب سياسات جامعة الملك فيصل، أو تأجيلها حتى يتم التحقق من الملف من قبل الموظف المسؤول أو وفقاً للسياسة المتبعة.

١٠- حجب رسائل البريد الإلكتروني المُرسلة إلى قائمة غير معرّفة من عناوين البريد الإلكتروني.

٢-٢ حماية المصادقة (Secure Authentication)

الهدف

ضمان حماية استخدام البريد الإلكتروني من خارج جامعة الملك فيصل من الوصول غير المصرّح به من خلال صفحة موقع البريد الإلكتروني (Webmail) أو برنامج قارئ البريد الإلكتروني الخارجي (Email Client).

المخاطر المحتملة

يُعرِّض الوصول غير المصرّح به إلى البريد الإلكتروني لجامعة الملك فيصل إلى مخاطر كبيرة قد تؤدي إلى سرقة المعلومات وانتحال الشخصيات مما يتيح استخدامها في تنفيذ المزيد من الهجمات السيبرانية ضد جامعة الملك فيصل وبنيتها التحتية.

الإجراءات المطلوبة

١- تطبيق آليات التحقّق من الهوية متعدّد العناصر "MFA" (Multi-Factor Authentication) على إمكانية وصول المستخدمين للبريد من خارج الشبكة خلال برنامج قارئ البريد الإلكتروني الخارجي (Email Client) وصفحة موقع البريد الإلكتروني (Webmail)، (مثل: "OWA" Outlook Web Access) وفقاً للضابط رقم ٢-٤-٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018).

٢- بالإضافة إلى ضرورة إدخال اسم المستخدم وكلمة المرور، يجب على المستخدم استعمال آليات أخرى للتحقّق من الهوية عند الدخول من خارج الشبكة، مثل: الخصائص الحيوية (Biometrics)، أو جهاز توليد الأرقام العشوائية (Hardware Keys)، أو الرسائل القصيرة المؤقتة لتسجيل الدخول (One-Time-Password)، أو البطاقات الذكية (Smartcards) أو شهادات التشفير (Certificates)، أو غيرها.

٣- ضبط متطلبّات إعدادات كلمات المرور المعقدة للبريد الإلكتروني وفقاً لسياسة إدارة هويات الدخول والصلاحيات المتّبعة في جامعة الملك فيصل.

٤- تطبيق تقنيات التشفير، مثل: «أمن مستوى النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks)، لحماية آليات التحقّق من الهوية خلال إرسالها. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suites) الموصي بها. يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة الملك فيصل.

٣-٢ حماية محتوى البريد الإلكتروني (Content Protection)

الهدف

ضمان حماية رسائل البريد الإلكتروني التي تحتوي على مرفقات من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقاً وأي نوع آخر من المرفقات الخبيثة.

المخاطر المحتملة

يُمكن أن ينخدع المستخدم برسائل البريد الإلكتروني التي تحتوي على مرفقات خبيثة حيث قد تتعرض جامعة الملك فيصل لاختراق بياناتها أو الوصول إليها بشكل غير مصرّح به أو كشفها في حال عدم فحص مرفقات البريد الإلكتروني.

الإجراءات المطلوبة

١- تطبيق وتفعيل تصنيفين لمرفقات البريد الإلكتروني: التصنيف الأول وفقاً لنوع الملف، والتصنيف الثاني وفقاً لمحتوى الملف.

٢- ترميز المرفقات حسب أنواع المرفقات وصيغتها. على سبيل المثال:

- **اللائحة السوداء:** جميع أنواع نسخ البرمجيات القابلة للتنفيذ من ويندوز (Windows PE) وأوامر ماكرو أوفيس (Office Macros) والبرمجيات أو الأوامر النصية (Scripts)، وغيره.
- **اللائحة الرمادية:** الأرشيفات متعدّدة المستويات (Multi-Layer Archives) وملفات حماية كلمة المرور وملفات التشفير والملفات التي يزيد حجمها عن الحد الأقصى، وغيرها من الملفات ضمن قائمة الحجر (Quarantine-list)
- **اللائحة البيضاء:** ملفات برامج أوفيس القياسية (مثل: docx وpptx وxlsx) وملفات pdf وtxt، والملفات الأرشيفية، وغيرها.
- **لائحة المرفقات غير المعروفة:** أنواع وصيغ الملفات غير المعروفة والتي يتعذّر التحقّق منها.

٣- ترميز جميع المرفقات بعد فحصها من البرمجيات الضارة بإدراج نتائج الفحص، على سبيل المثال:

- **ضارة:** تحتوي على فيروس، أو برنامج ضار، أو تهديد متقدّم مستمر، أو غيره.
- **آمنة:** تحتوي على ملف مرفق آمن.
- **غير معروفة:** أي تعذّر فحصها.

٤- تحديد أنواع الملفات باستخدام محتواها مثل ترويسة وتذييل الملف (Footer and Header) وليس من خلال صيغها.

٥- فحص جميع المرفقات المسموحة والتي تمت تصفيتها للتأكد من خلوها من الملفات الضارة، مثل: الفيروسات والبرمجيات الضارة وأي نوع آخر من الملفات المشبوهة.

٦- فحص جميع أنظمة وخوادم البريد للتحقّق من عدم وجود أي برمجيات ضارة أو مشبوهة في المكونات التقنية للبريد الإلكتروني وبوابة البريد (Mail Gateway) وخاصية ترحيل البريد (Mail Relay)، أو خادم البريد (Mail Server) قبل أن تصل إلى برنامج قارئ البريد (Email Client).

٧- إجراء فحص للتحقّق من عدم وجود أي برمجيات ضارة أو مشبوهة عبر برامج قراءة البريد (Email Clients) باستخدام حل يُقدّمه مورّد أو مزوّد مختلف عن الموجود في البند السابق مثل إضافة أدوات للحماية من الفيروسات إلى برنامج قارئ البريد.

٨- فحص جميع المرفقات المسموحة والتي تمت تصفيتها عبر إجراء تحليل ديناميكي للمرفقات باستخدام تقنية الحماية المعزولة (Sandbox) للتحقّق من التهديدات المتقدّمة المستمرة (APT) والبرمجيات الضارة غير المعروفة مسبقاً.

٩- حجب (أي عدم السماح لها بالمرور إلى بريد المستخدم) أو تجريد جميع رسائل البريد الإلكتروني التي تحتوي على ملفات مرفقة ضارة أو مصنفة ضمن اللائحة السوداء وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في جامعة الملك فيصل ثمّ إضافة عنوان المرسل والنطاق إلى اللائحة السوداء.

١٠- حجر (أي إيقاف وصولها إلى بريد المستخدم إلى حين التأكد من سلامة محتواها) جميع رسائل البريد الإلكتروني التي تتضمّن ملفات ضمن اللائحة الرمادية إذا كانت آمنة.

١١- حجر جميع رسائل البريد الإلكتروني التي تتضمّن ملفات مرفقة غير معروفة.

١٢- قبول جميع رسائل البريد الإلكتروني التي تتضمّن ملفات مرفقة آمنة ومسموحة.

٤-٢ التحقّق من مرسل البريد الإلكتروني (Email Sender Verification)

الهدف

ضمان توثيق نطاق البريد الإلكتروني للجامعة من خلال تحديد الخوادم المصرح لها بإرسال رسائل البريد الإلكتروني والتحقق من أن رسائل البريد الإلكتروني الواردة للجامعة مصدرها من نطاق موثوق به.

المخاطر المحتملة

تحمي خاصية التأكّد من سلامة وموثوقية رسائل البريد الإلكتروني جامعة الملك فيصل من عمليات تزوير البريد الإلكتروني والرسائل الإلكترونية الضارة والكشف عن المعلومات المهمّة والحسّاسة والوصول غير المصرّح به إلى الرسائل الإلكترونية الخاصة بالمستخدم.

الإجراءات المطلوبة

١- التحقّق من المُرسِل باختبار قاعدتين من بيانات سمعة المُرسِل (Sender Reputation) على الأقل.

٢- التحقّق من عنوان المُرسِل مقابل قوائم الرسائل الاقتحامية (Email SPAM lists) المتواجدة على الإنترنت والتي تحدث يومياً.

٣- التحقّق من بروتوكول الإنترنت ("IP" Internet Protocol) الخاص بخادم بريد المُرسِل واسم النطاق بمقارنته مع القائمة اللحظية لعناوين الإنترنت العشوائية (Real-time Blackhole Lists).

٥-٢ التحقّق من سلسلة الثقة المتعلقة بالبريد الإلكتروني (Email Chain of Trust Verification)

الهدف

ضمان الحفاظ على سريّة بيانات البريد الإلكتروني والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.

المخاطر المحتملة

قد يؤدي عدم التأكد من سلامة وموثوقية رسائل البريد الإلكتروني إلى عمليات تزوير البريد الإلكتروني والرسائل الإلكترونية الخبيثة والكشف عن المعلومات المهمة والحسّاسة والوصول غير المصرّح به إلى الرسائل الإلكترونية الخاصة بالمستخدمين.

الإجراءات المطلوبة

١- إنشاء وتسجيل إطار سياسة المُرسِل (Sender Policy Framework "SPF") والبريد المُعرَّف بمفاتيح النطاق (Domain Key Identified Mail "DKIM") ومصادقة الرسائل والإبلاغ عنها ومطابقتها استناداً إلى النطاق (Message Domain-based Authentication, Reporting and Conformance "DMARC").

٢- التحقّق من المُرسِل وفق نظام مصادقة هوية مُرسِل الرسائل (SenderID) وسجلات إطار سياسة المُرسِل (SPF) واتخاذ الإجراء المناسب وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في جامعة الملك فيصل.

- رفض الفشل الكامل (SPF Strict -Fail) في إطار سياسة المُرسِل.
- حجر الفشل الجزئي (SPF Relaxed -Fail) في إطار سياسة المُرسِل.

٣- التحقّق من المُرسِلين وفق البريد المُعرَّف بمفاتيح النطاق (DKIM) التي يستخدمونها.

- رفض الفشل في البريد المُعرَّف بمفاتيح النطاق.

٤- ضبط إطار سياسة المُرسِل (SPF) على السجلات الخارجية المقابلة لنظام أسماء النطاقات (External DNS Records) لكل أسماء النطاقات التي تملكها جامعة الملك فيصل للسماح فقط بسجلات تبادل البريد (Mail Exchange Records) في الخوادم التي صرّحت لها جامعة الملك فيصل بإرسال الرسائل الإلكترونية نيابةً عنها.

٥- ضبط سجلات البريد المُعرَّف بمفاتيح النطاق (DKIM) لتوقيع محتوى رسائل البريد الإلكتروني (Email Digital Signing) الخاصة بجامعة الملك فيصل وذلك بتحديد مفاتيح عامة تشفيرية للتواقيع (Public Key Cryptography).

٦- ضبط «مصادقة الرسائل والإبلاغ عنها ومطابقتها استناداً إلى النطاق» (DMARC) لأتمتة تطبيق الإجراءات المناسبة بشأن الأخطاء المرصودة في نظام مصادقة هوية مُرسِل الرسائل وسجلات إطار سياسة المُرسِل والبريد المُعرّف بمفاتيح النطاق وفقاً لسياسة حماية البريد الإلكتروني المتبعة في جامعة الملك فيصل. على سبيل المثال:

- **رفض/حجر** الفشل الجزئي (Relaxed Fail) في البريد المُعرَّف بمفاتيح النطاق (DKIM) وسجلات إطار سياسة المُرسِل (SPF).

ملاحظة: الفشل الجزئي (Relaxed Fail) يسمح بمرور الرسائل الواردة من النطاقات الفرعية، والفشل الكامل (Strict Fail) يمنع ذلك.

٦-٢ حماية أنظمة البريد الإلكتروني (Email Systems Security)

الهدف

ضمان حماية وأمن البنية التحتية الأساسية لخدمة البريد الإلكتروني بما في ذلك خوادم البريد وبواباته وقواعد بياناته وحلوله الأمنية.

المخاطر المحتملة

من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية البنية التحتية لخدمة البريد الإلكتروني في جامعة الملك فيصل إلى استغلال المهاجمين لنقاط الضعف الكامنة في أنظمة البريد الإلكتروني واستغلال ثغراتها للوصول غير المصرّح به إلى شبكة الجامعة وبياناتها.

الإجراءات المطلوبة

١- إجراء اختبارات أمنية دورية (مثل: فحص الثغرات الأمنية وتنفيذ عمليات اختبار الاختراق) وفقاً للسياسات والإجراءات ذات العلاقة في جامعة الملك فيصل.

٢- مراجعة وتطبيق حزم التحديثات والإصلاحات دورياً على أنظمة البريد الإلكتروني وفقاً لسياسة إدارة التحديثات والإصلاحات المتّبعة في جامعة الملك فيصل، وضمان تحديث جميع الأنظمة.

٣- حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من أنظمة البريد الإلكتروني، مثل: خدمات الطباعة وبروتوكول الاتصال عن بعد غير الآمن (Telnet)، وغيرها.

٤- ضبط إعدادات وتحصين (Secure Configuration and Hardening) أنظمة البريد الإلكتروني على مستوى التطبيقات وقاعدة البيانات والتشغيل كل ثلاثة أشهر. يُرجى الرجوع إلى معيار أمن الخادم ومعيار أمن قاعدة البيانات المعتمدين في جامعة الملك فيصل.

٥- تقييد الوصول (Restrict Access) إلى أنظمة البريد الإلكتروني ليكون مسموح به فقط لمديري أنظمة البريد الإلكتروني (Mail System Administrators).

٦- حذف أو إلغاء تفعيل الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة.

٧- إلزام مديري الأنظمة ومُشغّلي أنظمة البريد الإلكتروني باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى أنظمة البريد الإلكتروني.

٨- استخدام مبدأ الحماية الذي يمنح مديري ومُشغّلي أنظمة البريد الإلكتروني (Email System Administrators and Operators) الحد الأدنى من صلاحيات الوصول (Least-Privilege Principle) إلى مختلف أنواع أنظمة البريد الإلكتروني.

٩- تقييد الوصول الشبكي إلى أنظمة إدارة البريد الإلكتروني على المنطقة الشبكية التي تتواجد فيها والمنطقة الشبكية الخاصة بالإدارة (Management Zone).

١٠- حذف أو إلغاء تفعيل خصائص تطبيق البريد الإلكتروني وملفات الإعدادات غير الضرورية أو غير اللازمة.

١١- حجب إمكانية الوصول (Restrict Access) إلى مجلدات الشبكة (Network File Shares) والملفات غير الضرورية أو غير اللازمة.

١٢- استخدام ضوابط الأجهزة الطرفية (Peripheral Device Controls) وحجب الوصول إلى وسائل التخزين القابلة للإزالة مثل الأقراص المتحركة (CD) والأقراص المدمجة (DVD) وذاكرة التخزين (USB).

١٣- تثبيت برامج أنظمة البريد الإلكتروني على خوادم استضافة مخصصة لها.

١٤- ضبط رسائل خدمة برتوكولات نقل البريد (مثل: بروتوكول إرسال البريد البسيط "SMTP"، وبروتوكول مكتب البريد "POP"، وبروتوكول الوصول إلى رسائل الإنترنت "IMAP"، وغيرها) لمنع الكشف عن معلومات إصدار البرنامج أو نظام التشغيل (Exchange Version).

١٥- تفعيل أوامر البريد غير الخطرة فقط وذلك لتفادي الأوامر الخطرة مثل (VRFY وEXPN).

١٦- تفعيل سجلات الأحداث (Event Logging) في أنظمة البريد الإلكتروني وسجل التدقيق (Audit Log) الواجب إرسالهما إلى نظام مركزي لإدارة سجلات الأحداث وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني في جامعة الملك فيصل.

١٧- إنشاء البنية التحتية لخدمة البريد الإلكتروني باستخدام مبدأ المعمارية متعددة المستويات (Multi-Tier Architecture) المحمية باستخدام طبقتين مختلفتين من جدار الحماية (Firewalls). وتحديداً، إدراج بوابة أمن البريد الإلكتروني (Mail Gateway) في منطقة الإنترنت المحايدة (DMZ)، وخوادم تطبيقات البريد الإلكتروني في منطقة الإنتاج (Production Zone)، وخوادم قواعد بيانات البريد الإلكتروني في المنطقة الموثوقة (Trusted Zone) أو منطقة قاعدة البيانات (Database Zone).

١٨- حماية صفحة موقع البريد الإلكتروني خلف جدار حماية تطبيق الويب (Web Application Firewall "WAF").

١٩- تعطيل خاصية الترحيل المفتوح(Open Mail Relay) .

٢٠- ضبط تشفير نقل البريد الإلكتروني باستخدام تقنيات التشفير، مثل: «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية رسائل البريد الإلكتروني خلال إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suites) الموصي بها (مثل التشفير بمجموعة Suite B). يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة الملك فيصل.

٢١- ضبط مجموعات مواصفات الارتداد لبيانات البريد (Mail Bounce Profiles) على سبيل المثال، الارتداد القوي لرسائل البريد الإلكتروني المرسلة إلى عناوين بريد غير موجودة أو منتهية الصلاحية أو غير مفعّلة.

٧-٢ برنامج قارئ البريد الإلكتروني (Email Client Security)

الهدف

ضمان حماية استخدام البريد الإلكتروني من خلال صفحة موقع البريد الإلكتروني (Webmail) أو برنامج قارئ البريد الإلكتروني (Email Client).

المخاطر المحتملة

من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية برنامج قارئ البريد الإلكتروني إلى مخاطر كبيرة قد تؤدي إلى سرقة المعلومات وانتحال الشخصيات مما يتيح استخدامها في تنفيذ المزيد من الهجمات الضارة ضد موظفي جامعة الملك فيصل وبنيتها التحتية.

الإجراءات المطلوبة

١- استخدام برنامج قارئ بريد إلكتروني مرخص وموثوق.

٢- منع تشغيل صفحة موقع البريد الإلكتروني على المتصفحات غير المرخصة.

٣- تعطيل التطبيقات الإضافية أو المكونات غير الضرورية أو غير المسموح بها لبرنامج قارئ البريد الإلكتروني.

٤- منع تشغيل لغات البرمجة النصية في برنامج قارئ البريد الإلكتروني.

٥- ضبط تكامل برنامج قارئ البريد الإلكتروني مع أنظمة حماية الأجهزة كمضاد الفيروسات والبرمجيات الضارة.

٨-٢ النسخ الاحتياطية والأرشفة (Backup and Archival)

الهدف

ضمان سلامة بيانات البريد الإلكتروني وتوافرها وقابلية استعادتها وحمايتها من فقدانها أو تخريبها.

المخاطر المحتملة

في حال حذف بيانات البريد الإلكتروني والرسائل الإلكترونية أو العبث بها أو فقدانها بالخطأ أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن جامعة الملك فيصل من استرداد بيانات بريدها الإلكتروني وسجل اتصالاتها مما يؤثّر على أنشطة أعمالها الاعتيادية.

الإجراءات المطلوبة

١- إجراء عمليات نسخ احتياطية دورية كاملة لخوادم وقواعد بيانات البريد الإلكتروني وفقاً لسياسة إدارة النسخ الاحتياطية، ويشمل ذلك النسخ الاحتياطية لأنظمة تشغيل الخوادم وإعدادات تطبيق البريد وقاعدة البيانات بالإضافة إلى مجمل قواعد البيانات وصناديق البريد، وإضافة ترتيب تسلسلي للنسخ الاحتياطية لنظام البريد الإلكتروني ومحتويات البريد الخاصة بجامعة الملك فيصل وتسجيل وقتها، وتاريخها، وجدولتها.

٢- إجراء عملية نسخ احتياطي إضافية يومياً أو وفقاً لسياسة إدارة النسخ الاحتياطية لمحتويات بريد المستخدمين.

٣- تشفير النسخ الاحتياطية لنظام البريد الإلكتروني ومحتويات البريد وفقاً لسياسة التشفير المعتمدة في جامعة الملك فيصل.

٤- تخزين النسخ الاحتياطية لنظام البريد الإلكتروني ومحتويات البريد الخاصة بجامعة الملك فيصل في موقعين محميّين منفصلين على الأقل وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة الملك فيصل.

٥- تطبيق إجراءات توثيق وسلامة (Integrity Verification) النسخ الاحتياطية لضمان نسخ بيانات البريد الإلكتروني أو أرشفتها بطريقة صحيحة.

٦- تجربة استعادة جميع أنواع النسخ الاحتياطية دورياً لضمان سلامة عملية النسخ الاحتياطي وفقاً لسياسة إدارة النسخ الاحتياطية.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٣. معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني

الأهداف

يهدف هذا المعيار إلى توفير متطلبات الأمن السيبراني التقنية المبنية على أفضل الممارسات والمعايير لإدارة سجلات الأحداث ومراقبة الأمن السيبراني والعمل على حماية جامعة الملك فيصل من التهديدات الداخلية والخارجية.

يتبع هذا المعيار المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهو متطلب تشريعي في الضابط رقم ١-٣-٣ والضابط رقم ٢-١٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع تقنيات إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) في جامعة الملك فيصل، وينطبق على جميع العاملين في جامعة الملك فيصل.

المعايير

٣-١ صيغة السجل (Log Format)

الهدف

استخدام صيغة قياسية ومتسقة للسجل تشتمل على جميع المعلومات المطلوبة.

المخاطر المحتملة

قد يصعب الربط بين عدة سجلات مختلفة إذا تم حفظها بصورة غير متسقة، وهذا يؤدي إلى زيادة المخاطر الناتجة عن المعلومات الخاطئة، وبالتالي يُعقِّد التعامل مع الأحداث الأمنية وحلها.

الإجراءات المطلوبة

١- يجب أن تشتمل صيغة سجل الأحداث على المعلومات التالية:

١-١ **نوع سجل الأحداث:** مثل النظام، والأمن، والتدقيق، والنقطة الأساسية (Kernel)، والتصريح، والبريد، وغيرها.

١-٢ **موقع** الحدث أو مصدر السجل ونظامه.

١-٣ **تاريخ** سجل الحدث **وختمه الزمني.**

١-٤ **حالة الحدث:** مثل ناجح، أو فاشل، أو نشط، أو غير نشط، أو مسموح، أو مرفوض، أو غيره.

١-٥ **مستوى خطورة الحدث:** مثل طارئ، أو تنبيه، أو حرج، أو خطأ، أو تحذير، أو إشعار معلوماتي، أو إشعار تصحيحي.

١-٦ **رسالة الحدث:** رسالة فعلية من الحدث.

٢- إدراج تفاصيل إضافية في السجلات حيثما ينطبق ذلك، مثل: المستخدم وعنوان الإنترنت ومنفذ المصدر، وعنوان ومنفذ الوجهة، وعناصر أخرى مفيدة.

٣-٢ الأختام الزمنية (Timestamps) - الخوادم الزمنية المتزامنة الإضافية (Synchronized Redundant Time Servers)

الهدف

استخدام نظام زمني ثابت للأصول المعلوماتية والتقنية الداخلية.

المخاطر المحتملة

قد يصعب المقارنة بين مجموعتين مختلفتين من السجلات إذا تم حفظها بصورة غير متسقة، ويؤدي ذلك إلى زيادة المخاطر الناتجة عن المعلومات الخاطئة وبالتالي يُعقِّد التعامل مع الأحداث الأمنية وحلها.

الإجراءات المطلوبة

تزامن الأصل المعلوماتي والتقني مع ثلاثة خوادم زمنية إضافية على الأقل في غضون أجزاء من الثانية.

٣-٣ تسجيل الأحداث (Event Logging)

الهدف

التأكّد من توثيق وتسجيل الأحداث السيبرانية والأنشطة غير المصرّح بها التي تشهدها البيئة.

المخاطر المحتملة

من الضروري تسجيل بعض الأحداث الأساسية التي تُنفذ في البيئة، وإذا تعذّر على جامعة الملك فيصل تسجيل الأحداث التي حدّدتها متطلّبات الضابط، فسيؤدي ذلك إلى زيادة المخاطر الناتجة عن الأحداث غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في البيئة، والتي قد تؤثّر على أعمال جامعة الملك فيصل بناءً على مستوى خطورة الحدث.

الإجراءات المطلوبة

تسجيل جميع الأحداث المُحدّدة في متطلّبات هذا المعيار والتي تشمل:

- محاولات الدخول الناجحة.
- محاولات الدخول غير الناجحة، بالإضافة إلى تحديد ما إذا كانت محاولة الدخول قد تضمّنت إدخال كلمة مرور خاطئة.
- جميع عمليات تسجيل الخروج.
- الإضافات والمحذوفات والتعديلات على حسابات وصلاحيات المستخدم.
- تغيير المستخدم لهويته خلال فترة زمنية معيّنة على الإنترنت.
- محاولات لتنفيذ مهام غير مصرّح بها.
- أنشطة الحسابات التي تملك صلاحيات هامة وحسّاسة.
- إجراء تعديلات على إعدادات النظام (محدّدات النظام).
- حق الوصول لقراءة أو تعديل معلومات سريّة للغاية التي يُحتمل تعرّضها للسرقة.
- تسريب مواد متعلّقة بمعلومات سريّة للغاية خارج جامعة الملك فيصل.
- الأحداث المتعلقة بالاتصالات الواردة والصادرة والتي تتضمّن أنشطة غير عادية أو غير مصرّح بها بما في ذلك وجود برامج ضارة (رموز البرامج الخبيثة "Malicious Code" وبرامج التجسّس "Spyware" والبرامج الدعائية "Adware").
- الإضافات والمحذوفات والتعديلات على معايير سجل الأمن والتدقيق.
- الأخطاء (أي المشاكل التقنية في الأصول المعلوماتية والتقنية) التي قد تحدث نتيجة حادث أمني.
- تشغيل الأنشطة أو إيقافها عن طريق خدمة معيّنة.
- تعطّل النظام أو إعادة تشغيله.

- تغيير كلمة المرور.
- تفعيل جميع السجلات للأنظمة الحسّاسة.

٤-٣ مصادر الأحداث (Event Sources)

الهدف

التأكّد من مراقبة جميع سجلات الأحداث المتعلّقة بالأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل لكشف أي نشاط غير مصرّح به في الشبكة والذي قد يتسبب بحدث أمني.

المخاطر المحتملة

إن عدم التمكّن من كشف أي نشاط غير مصرّح به والذي يمكن اكتشافه ضمن سجلات الأحداث قد يؤدي إلى احتمالية الاستجابة أو التعامل مع هذا الخطر بطريقة غير مناسبة، لذا من المهم الكشف المبكر عن تلك المخاطر حتى لا تصبح أكثر خطورة.

الإجراءات المطلوبة

١- تهيئة مصادر سجل الأحداث وأنظمة تسجيل الدخول لنقل السجلات عبر بروتوكولات موثوقة وشائعة الاستخدام لنقل سجل الأحداث، مثل: (Syslog)، و(Windows Instrumentation Interface)، و(SNMP Traps)، وغيرها.

٢- جمع كافة سجلات الأحداث من المصادر المُحدّدة ضمن هذا المطلب:

- الأنظمة بما فيها أنظمة التشغيل وقواعد البيانات ووسائط التخزين والشبكات والتطبيقات، التي تغطي أحداث النظام وسجلات الأمن والتدقيق.
- الأنظمة الحسّاسة بما فيها أنظمة التشغيل وقواعد البيانات ووسائط التخزين والشبكات والتطبيقات، التي تغطي أحداث النظام وسجلات الأمن والتدقيق.
- أحداث الحسابات ذات الصلاحيات الهامة والحسّاسة.
- الأحداث الخاصة بالتصفّح والاتصال بالإنترنت والشبكة اللاسلكية.
- الأحداث الناتجة عن نقل البيانات إلى وسائط تخزين خارجية.
- سجلات الأحداث الصادرة من تقنيات إدارة تغييرات الملفات (Monitoring File Integrity).
- سجلات الأحداث المُولّدة من تغييرات إعدادات النظام وتحديثات وإصلاحات النظام والتغييرات على التطبيقات.
- أنشطة مشبوهة مثل الأنشطة التي يكتشفها نظام منع الاختراقات (Prevention System Intrusion).
- أحداث تُولّدها الحلول الأمنية بما فيها البرامج المضادة للبرمجيات الخبيثة (Antivirus, Antimalware, Advanced Persistent Threat "APT") وتقنيات الوصول عن بُعد (Remote-Access Technologies) (مثل: الشبكة الافتراضية الخاصة "Virtual Private Network")، ووسطاء الويب (Web Proxies)، وبرنامج إدارة الثغرات، ونظام منع الاختراقات في المستضيف (Host System Intrusion Prevention)، وخوادم التحقّق من الهوية (Authentication Servers)، وغيرها.

- أحداث تُولّدها أجهزة حماية الشبكة بما في ذلك جدران الحماية والمُوجّهات (Routers) ومديري حركة الشبكة (Traffic Managers)، وغيرها.
- أحداث تُولّدها البيئة الافتراضية وأدواتها وبنيتها التحتية الأساسية.
- تفعيل تسجيل الاستفسارات (Query Logging) في نظام أسماء النطاقات (Domain Name System) حيثما أمكن ذلك من الناحية التقنية.
- سجلات الأحداث التي تُولّدها أنظمة التحكّم الصناعي (Systems Industrial Control).

٣-٥ مراقبة الأحداث (Events Monitoring)

الهدف

كشف أي نشاط غير مصرّح به في الشبكة والذي قد يسبب حدث أمني.

المخاطر المحتملة

إن عدم التمكّن من كشف أي نشاط غير مصرّح به في الشبكة يمنع جامعة الملك فيصل من التعامل بالطريقة المناسبة مع الأحداث المشبوهة قبل أن تتفاقم وتصبح أكثر خطورة.

الإجراءات المطلوبة

١- يجب مراجعة تنبيهات الأحداث الأمنية الناتجة عن جدران الحماية يومياً للكشف عن أي محاولات وصول غير مصرح بها أو سلوك غير عادي. وتستطيع جامعة الملك فيصل مراقبة التنبيهات الصادرة عن جدران الحماية على سبيل المثال من خلال مراقبة السجلات يومياً أو من خلال مراقبة جوانب النظام الأخرى مثل أنماط محاولة الوصول، وخصائص الوصول، وغيرها من الإجراءات.

٢- تفعيل مراقبة الشبكة اللاسلكية وذلك لكشف نقاط الوصول اللاسلكية غير المصرّح بها. وقد تتجاوز الإشارات اللاسلكية حدود النطاق الخاضع للمراقبة، وعلى ذلك تتخذ الجهات خطوة استباقية للبحث عن الاتصالات اللاسلكية غير المصرّح بها، بما في ذلك إجراء عمليات مسح مكثّفة عن نقاط الوصول اللاسلكية غير المصرّح بها، وهذه العمليات المسحية لا تقتصر فقط على الأصول التي تحتوي على أصول معلوماتية وتقنية، بل تشمل كذلك المناطق الواقعة خارج مبانيها عند الضرورة، وذلك للتحقّق من عدم اتصال نقاط الوصول اللاسلكية غير المصرّح بها بالأنظمة.

٣- تطبيق آليات مراقبة المستضيف (Host-based Monitoring Mechanisms) على النهايات الطرفية للأصول المعلوماتية والتقنية ذات الخطورة العالية. وتشمل مكوّنات الأصول المعلوماتية والتقنية التي يُمكن تطبيق آليات مراقبة المستضيف عليها الخوادم وأجهزة المستخدمين والأجهزة المحمولة.

٤- تطبيق آليات المراقبة القائمة على ملف تعريف الملف والسلوك (Behavior-based Code Signature-based and)، مثل البرامج المضادة للفيروسات وتقنية كشف النهايات الطرفية والاستجابة لها (Endpoint Detection and Response) وأدوات كشف التهديدات المتقدمة المستمرة (APT Tools) على الأصول المعلوماتية والتقنية لكشف رمز البرامج الخبيثة.

٥- ضمان مواصلة تحديث آليات المراقبة القائمة على ملفات التعريف والسلوك بشكل مستمر.

٦- تُنشَر أجهزة المراقبة لمتابعة الاتصالات على المكوّنات الخارجية للنظام (مثل: محيط النظام) وعلى المكوّنات الداخلية الرئيسية (مثل: الواجهات المنطقية والمادية داخل الأصول المعلوماتية والتقنية) لاكتشاف العيوب واكتشاف التسريب المخفي للمعلومات وتتبع أنواع محدّدة من الأنشطة التي تهم جامعة الملك فيصل، على سبيل المثال الأجزاء الشبكية حيث تقع الأنظمة التي يُمكن الوصول إليها من الإنترنت.

٧- تطبيق أدوات المراقبة للكشف عن مؤشرات الهجمات المنفّذة ضد الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل والتي تؤدي إلى حجب الخدمة.

٦-٣ التنبيه بالأحداث (Event Alerting)

الهدف

التأكّد من تفعيل وضبط خاصية التنبيه بالأحداث وإبلاغ العاملين المعنيين في جامعة الملك فيصل بشأنها ليتمكّنوا من التعامل مع أي حادث أمني بأكبر قدر من الفاعلية.

المخاطر المحتملة

قد يؤدي عدم ضبط خاصية التنبيه بالأحداث في أنظمة التسجيل إلى التعامل مع الأحداث الأمنية بطريقة خاطئة أو حتّى عدم التعامل معها كلياً.

الإجراءات المطلوبة

١- إصدار التنبيهات للأصول المعلوماتية والتقنية عند وقوع أحداث المراقبة الأمنية المحدّدة مسبقاً و/أو عند استيفاء مستويات المؤشرات المتعلّقة بأي نشاط ضار محتمل.

٢- ضبط وسائل التنبيه لإبلاغ العاملين المعنيين، بما في ذلك البريد الإلكتروني والرسائل النصية القصيرة وأنظمة شاشات المراقبة، وغيرها.

٧-٣ مستويات التنبيه (Alert Threshold)

الهدف

اتباع نهج مُوثّق بشأن الحالات التي ينبغي تشغيل التنبيهات فيها.

المخاطر المحتملة

قد يؤدي عدم توثيق نطاق التنبيهات والغرض منها إلى عدم تهيئتها بالشكل المناسب، وقد تمر الأحداث الضارة المحتملة دون أن يلاحظها أحد.

الإجراءات المطلوبة

تحديد وتوثيق المستويات المحدّدة للتنبيه عن أحداث مراقبة الأمن، ومراجعة مستوى التنبيه وتحديثه دورياً لمواكبة الهجمات الأمنية المستجدة.

٣-٨ التنبيه بالأحداث الناتجة عن جدار الحماية (Firewall Event Alerting)

الهدف

إبلاغ العاملين المعنيين المؤهلين للتعامل مع الأحداث الأمنية المحتملة والناتجة عن جدران الحماية.

المخاطر المحتملة

إن لم يتم إبلاغ العاملين المعنيين بالأحداث الناتجة عن جدار الحماية، فإن جامعة الملك فيصل لن تكون على دراية بالمحاولات الخبيثة المحتملة غير المصرّح بها للاتصال بالشبكة، وبالتالي إذا تمكّن هذا النشاط من اختراق جدار الحماية، ستتعرّض أعمال جامعة الملك فيصل لمخاطر ضارة ناتجة عن الحادث الأمني.

الإجراءات المطلوبة

ضبط التنبيهات أو أدوات المراقبة لتنويه العاملين المعنيين بالأحداث المتعلّقة بالأمن والناتجة عن جدار الحماية.

٣-٩ التنبيه بالأحداث الناتجة عن التطبيقات (Application Event Alerting)

الهدف

التأكّد من توثيق وتسجيل الأحداث الأمنية والأنشطة غير المصرّح بها التي تشهدها البيئة.

المخاطر المحتملة

من الضروري تسجيل بعض الأحداث المحورية المتعلّقة بالتطبيقات الخاصة بجامعة الملك فيصل، فإذا تعذّر على جامعة الملك فيصل تسجيل الحوادث المتعلّقة بالتطبيق والتي حدّدتها متطلّبات الضابط، سيؤدي ذلك إلى زيادة المخاطر الناتجة عن الحوادث الأمنية غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في التطبيق، والتي قد تؤثّر على أعمال جامعة الملك فيصل بناءً على مستوى خطورة الحادث.

الإجراءات المطلوبة

١- تسجيل جميع طلبات العميل واستجابات الخادم.

٢- تسجيل جميع معلومات الحساب (مثل: محاولات التحقّق الناجحة وغير الناجحة والتغييرات على الحساب).

٣- تسجيل جميع المعلومات المتعلّقة بالاستخدام (مثل: عدد الأنشطة التي تحدث في فترة معيّنة).

٤- تسجيل جميع الإجراءات التشغيلية المهمّة (مثل: تشغيل وإغلاق التطبيقات وأعطال التطبيقات والتغييرات على إعدادات التطبيقات).

٣-١٠ مراقبة البرمجيات الضارة في الاتصالات (Malware in Communication Monitoring)

الهدف

تحديد وجود البرمجيات الضارة (مثل: رمز البرامج الخبيثة وبرامج التجسّس والإعلانات المتسلّلة) في اتصالات جامعة الملك فيصل قبل أن تتسبّب بأي ضرر.

المخاطر المحتملة

إذا لم يتم كشف أي استخدام غير مصرّح به للأنشطة بما في ذلك وجود البرمجيات الضارة، لن تكون جامعة الملك فيصل على دراية بوجود البرمجيات الضارة قبل أن تنتشر، مما يعرّض عملها لخطر هجوم أمني واسع النطاق.

الإجراءات المطلوبة

١- مراقبة الاتصالات الواردة والصادرة الخاصة بجامعة الملك فيصل (مثل: رسائل البريد الإلكتروني والملفات المرفقة وعمليات التحميل) لضمان خلوها من البرمجيات الضارة (مثل: البرمجيات الضارة وبرامج التجسّس والبرامج الدعائية).

٣-١١ تحليلات مراجعة سجل الأحداث (Event Log Review Analytics)

الهدف

يُمكن أن يسهم تحليل السجل ونظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) في اكتشاف الأنشطة المشبوهة وتعزيز قدرات الاستجابة لحوادث الأمن السيبراني وكشف الهجمات التي تجاوزت الأنظمة الأمنية الأخرى.

المخاطر المحتملة

إن عدم التمكّن من كشف أحداث وحوادث الأمن السيبراني سيزيد من المخاطر الناتجة عن عدم ملاحظة الهجمات السيبرانية مما يؤدي إلى انتهاك الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل.

الإجراءات المطلوبة

١- إرسال جميع الأحداث إلى نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني من أجل إدارة السجلات وتحليل محتواها وعلاقتها ببعضها والتنبيه عليها.

٢- إجراء مراجعة دورية لسجلات الأحداث لمراقبة السلوكيات والأحداث المشبوهة واكتشافها.

٣- ضبط نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني دورياً لتحديد الأحداث القابلة للتطبيق وتقليل الأحداث الناتجة عنها بطريقة أفضل.

٤- مراجعة سجلات الأحداث والتنبيهات دورياً باستخدام أساليب يدوية وتقنيات آلية.

٥- الكشف عن الأحداث غير المصرّح بها والمتعلّقة بالأصول المعلوماتية والتقنية.

٦- كشف سوء استخدام حسابات المستخدم ذات الصلاحيات الهامة والحسّاسة.

٣-١٢ تحويل السجل وتحليله (Log Conversion and Parsing)

الهدف

التأكّد من مراقبة جميع سجلات الأحداث المتعلّقة بالأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل لكشف أي نشاط غير مصرّح به في الشبكة والذي قد يسبب حدثاً أمنياً.

المخاطر المحتملة

من الضروري تسجيل بعض الأحداث المحورية التي تُنفذ في البيئة، فإذا تعذّر على جامعة الملك فيصل تسجيل الأحداث التي حدّدتها متطلّبات الضابط، سيؤدي ذلك إلى زيادة المخاطر الناتجة عن الأحداث غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في البيئة، والتي قد تؤثّر على أعمال جامعة الملك فيصل بناءً على مستوى خطورة الحادث.

الإجراءات المطلوبة

١- استخدام أدوات لتحويل السجلات غير المدعومة من نظام التسجيل الخاص بجامعة الملك فيصل إلى صيغة قياسية أو مدعومة للسجل.

٢- تطبيق برنامج تسجيل مزوّد بآليات التحليل لاسترجاع السجلات من الأنظمة غير المدعومة بطريقة مناسبة.

٣-١٣ المراقبة المستمرة (Continuous Monitoring)

الهدف

تفعيل المراقبة المستمرة لجميع سجلات الأصول المعلوماتية والتقنية للكشف عن الأنشطة الخبيثة والحفاظ على فاعلية المراقبة مع الوقت.

المخاطر المحتملة

إذا لم تضع جامعة الملك فيصل خطّة مراقبة لهذه الأنشطة وتوثّقها، فقد يرتفع خطر عدم وجود مراقبة مخصصة أو كافية لهذا الغرض، مما يزيد من مخاطر عدم الكشف عن الأنشطة الخبيثة.

الإجراءات المطلوبة

١- تطوير وإعداد خطّة للمراقبة المستمرة (والتي تشمل على سبيل المثال: الجوانب التي يجب مراقبتها في نطاق العمل، وآلية المراقبة، واختبار فاعلية المراقبة) للأصول المعلوماتية والتقنية وتحديثها عند الحاجة.

٣-١٤ أمن نظام التسجيل (Logging System Security)

الهدف

ضمان حماية وأمن البنية التحتية الأساسية لنظام التسجيل بما في ذلك محرّكات جمع سجلات الأحداث وتجميعها وربطها.

المخاطر المحتملة

من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية البنية التحتية لنظام التسجيل في جامعة الملك فيصل إلى استفادة المهاجمين من نقاط الضعف الكامنة في أنظمة التسجيل واستغلال ثغراتها للوصول غير مصرّح به إلى شبكة الجامعة وبياناتها.

الإجراءات المطلوبة

١- إجراء اختبارات أمنية دورية (مثل: تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في جامعة الملك فيصل.

٢- تنفيذ إصلاحات وتحديثات دورية على أنظمة التسجيل وفقاً لسياسة إدارة التحديثات والإصلاحات المتّبعة في جامعة الملك فيصل، وضمان تحديث جميع الأنظمة.

٣- حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من أنظمة التسجيل (مثل: خدمات الطباعة وبروتوكول تل نت "Telnet"، وغيرها).

٤- ضبط وتحصين أنظمة التسجيل بما في ذلك التطبيقات وقاعدة البيانات والتحصين على مستوى نظام التشغيل. يُرجى الرجوع إلى معيار أمن الخادم ومعيار أمن قاعدة البيانات المعتمدين في جامعة الملك فيصل.

٥- تقييد الوصول لأنظمة التسجيل وحصره على مديري نظام التسجيل فقط.

٦- حذف أو إلغاء تفعيل الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة.

٧- إلزام مشرفي ومُشغّلي أنظمة التسجيل باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى أنظمة التسجيل.

٨- استخدام مبدأ الحد الأدنى من الصلاحيات والامتيازات الذي يمنح مديري ومُشغّلي أنظمة التسجيل امتيازات الوصول إلى مختلف أنواع أنظمة التسجيل.

٩- تقييد الوصول لأنظمة التسجيل من خلال المنطقة الإدارية أو الشبكة المحلية الافتراضية الإدارية (Management VLAN) فقط.

١٠- حذف أو إلغاء تفعيل خصائص نظام التسجيل وملفات الإعدادات غير الضرورية أو غير اللازمة.

١١- حجب إمكانية الوصول إلى الملفات المشتركة عبر الشبكة والملفات غير الضرورية أو غير اللازمة.

١٢- استخدام ضوابط الأجهزة وحجب الوصول إلى وسائط التخزين القابلة للإزالة.

١٣- تثبيت برامج أنظمة تسجيل الأحداث على خوادم مخصصة لها.

١٤- استخدام محرّك لجمع الأحداث في كل منطقة من مناطق بنية الشبكة، والسماح فقط لهذه المحرّكات بالتواصل مع نظام التسجيل المركزي أو أنظمة تجميع السجلات، على أن تتوفر في المناطق التالية على الأقل:

- وضع محرّك لجمع الأحداث في المنطقة المحايدة (DMZ).
- وضع محرّك لجمع الأحداث في منطقة قاعدة البيانات.
- وضع محرّك لجمع الأحداث في منطقة التطبيقات.
- وضع محرّك لجمع الأحداث في منطقة خدمات المؤسسة.
- وضع محرّك لجمع الأحداث في منطقة المستخدم.

- وضع محرّك لجمع الأحداث في منطقة الإدارة.

١٥-٣ اختبار ومراجعة نظام المراقبة (Monitoring System Testing and Review)

الهدف

الحفاظ على القدرات التشغيلية والفاعلية في الكشف عن المحاولات غير المصرّح بها للوصول إلى الأصول المعلوماتية والتقنية.

المخاطر المحتملة

إذا لم تنجح أنظمة المراقبة في الكشف عن الأنشطة غير المصرّح بها، فإن ذلك سيزيد من احتمالية عدم ملاحظة النشاط الخبيث، والذي قد يؤدي إلى وقوع حادث أمني خطير.

الإجراءات المطلوبة

١- إجراء مراجعات واختبارات على أدوات المراقبة الأمنية الخاصة بجامعة الملك فيصل عن طريق أفراد مصرّح لهم بذلك للتأكّد من الالتزام بسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة في جامعة الملك فيصل ونجاحها في تلبية أهداف المراقبة.

١٦-٣ الاحتفاظ بسجلات الأحداث (Retaining Event Logs)

الهدف

تجنّب حذف سجلات الأحداث الأمنية خلال الفترة التي يُمكن أن تُستخدَم خلالها.

المخاطر المحتملة

إذا حُذِفَت سجلات الأحداث الأمنية قبل تدقيقها أو التحقيق فيها، لن تتمكّن جامعة الملك فيصل من حماية أو فحص الأنشطة التي حدثت في الأصول المعلوماتية والتقنية الخاصة بها.

الإجراءات المطلوبة

١- القيام بالنسخ الاحتياطي للسجلات دورياً ووفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة الملك فيصل.

٢- الاحتفاظ بسجلات الأحداث لمدة ١٢ شهراً على الأقل، ولمدة ١٨ شهراً بالنسبة للأصول الحسّاسة كحد أدنى أو لفترة أطول، وفقاً لسياسة الأمن السيبراني المعتمدة في جامعة الملك فيصل.

٣- تقييد أرشفة وحذف سجلات الأحداث وحصره على المستخدمين المصرّح لهم وذلك فقط بعد انتهاء المدّة الزمنية المحدّدة للاحتفاظ بالسجلات، والسماح للمديرين المعنيين بالأصول المعلوماتية والتقنية بإجراء عملية أرشفة سجلات الأحداث وحذفها.

٤- اختبار إمكانية استعادة واسترجاع النسخ الاحتياطية دورياً وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة الملك فيصل.

١٧-٣ توفير عملية بديلة لتسجيل الأحداث (Alternate Logging Capability)

الهدف

تمكين جامعة الملك فيصل من مواصلة تسجيل الأنشطة المتعلّقة بالأحداث الأمنية الحسّاسة حتّى في حال تعطّل الوسيلة الأساسية لتسجيل الأحداث (مثل: التسجيل المركزي).

المخاطر المحتملة

إذا تعطّلت وسيلة تسجيل الأحداث الأساسية المتعلّقة بأصل عالي الخطورة ولم تتوفّر عملية تسجيل بديلة، فإنه قد يتعذّر إنشاء سجل تدقيق أو تحديد النشاط الخبيث وذلك لعدم وجود سجلات يُمكن أن تستخدمها جامعة الملك فيصل للقيام بإجراءات المراقبة والتحقيق، علماً بأن الأصول الأعلى خطورة تؤثّر بشكل أكبر على أعمال جامعة الملك فيصل في حال وقوع حادث أمني معيّن.

الإجراءات المطلوبة

ضبط الأنظمة الحساسة، بالإضافة إلى إرسال السجلات إلى نظام تسجيل أحداث مركزي، لتحفظ سجلات الأحداث على أجهزتها في حال تعطّل الاتصال بالشبكة.

٣-١٨ توافر سجل الأحداث (Event Log Availability)

الهدف

ضمان استمرارية تشغيل وسيلة تسجيل الأحداث وقابلية استخدامها للأصول المعلوماتية والتقنية الحسّاسة.

المخاطر المحتملة

إذا لم تتوفّر وسيلة تسجيل الأحداث، فإن ذلك سيزيد من احتمالية عدم ملاحظة النشاط الخبيث وعدم القدرة على إجراء تحقيق بشأن الحادث والذي قد يؤدي إلى وقوع حادث أمني خطير.

الإجراءات المطلوبة

١- ضبط الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل والتي تحتوي على معلومات محمية، أو معلومات مصنفة من خلال تقييم إدارة المخاطر على أنها تتطلب تسجيل أحداثها، لإرسال الأحداث الخاصة بها بشكلٍ دائم.

٢- إعداد أنظمة تسجيل إضافية متعدّدة مزوّدة بقدرات توفير الخدمة على مدار الساعة ودون انقطاع.

٣-١٩ تصنيف السجلات (Log Classification)

الهدف

يجب حماية جميع سجلات أحداث الأمن السيبراني بطريقة آمنة.

المخاطر المحتملة

إذا طبّقت السجلات ضوابط مُخصّصة لبيانات ذات تصنيف أدنى على الرغم من احتواء هذه السجلات على بيانات مُصنّفة بأنها سريّة للغاية، فستكون هذه البيانات أكثر عرضة لخطر انتهاكها لأن الضوابط المحدّدة لحمايتها تعتبر أقل صرامة.

الإجراءات المطلوبة

١- التعامل مع أنظمة التسجيل المركزي باعتبار أنها تحتوي بحدٍّ أدنى على بيانات **سرية ومقيدة** خاصة بجامعة الملك فيصل وأنها ملتزمة بجميع الضوابط ذات العلاقة بسريّة المعلومات.

٢- بالنسبة إلى أي سجل للتطبيقات أو للأنشطة يحتوي على بيانات مُصنّفة على أنها **سرية للغاية**، يجب فرض الضوابط المطلوبة لهذا النوع من البيانات.

٣-٢٠ أمن السجلات وسلامتها (Log Integrity and Security)

الهدف

اعتماد آلية قادرة على كشف التعديلات على سجلات الأحداث الأمنية للتأكد من الاحتفاظ بها في حالتها الأصلية.

المخاطر المحتملة

إذا كان من الممكن تعديل سجلات الأحداث الأمنية دون وجود أي وسيلة لكشف هذا التعديل، فيمكن للمستخدم أن يُخفي نشاطه الخبيث داخل الأصل المعلوماتي والتقني. وفي هذه الحالة، إذا أُجري تحقيق بناءً على الأنشطة الضارة التي قام بها المستخدم، فلن يكون هناك دليل لمحاكمة المستخدم، ولن تُوجّه جامعة الملك فيصل ادعاءات مبرّرة بحق المستخدم ذي النوايا الضارة أو الخبيثة. كما أنه في حال انتهاك سلامة السجلات، فإنها قد تعتبر غير مقبولة في إجراءات المحكمة.

الإجراءات المطلوبة

١- الحفاظ على سلامة السجل الأصلي، وتوفير آليات لحماية سلامة السجل بما فيها ضابط تقييد الوصول ومستودعات البيانات المحظورة، وغيرها.

٢- تطبيق وسائل لتشفير السجلات في حالتي الإرسال والتخزين، مثل أمن طبقة النقل (Transport Layer Security)، واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) المُوصي بها (مثل: التشفير بمجموعة suite B). يُرجى الرجوع إلى المعيار رقم (١٢) – معيار التشفير بالقسم الثالث من هذه الوثيقة.

٣- تطبيق وسائل يُمكنها كشف التعديلات على السجلات في حالتي الإرسال والتخزين مثل خوارزميتي دالة التجزئة (Hashing) واختزال الرسالة (Message Digest) التشفيريتين، وذلك بالإضافة إلى آليات لكشف التعديل أو محاولات التعديل التي تعتمد على أساليب معيّنة مثل تقليل حجم السجل وتغيير دالة تجزئة الملف ووصول العمليات من غير النظام (مثل: كافة العمليات لكتابة واختزال السجلات باستثناء الآلية منها). يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة الملك فيصل للاطلاع على متطلّبات السلامة والتجزئة.

٤- تقييد الوصول إلى ملفات السجل ووسائط تخزين السجلات على نظام التسجيل فقط. ومنح المديرين حق الوصول إلى السجلات لأغراض استكشاف الأخطاء وإصلاحها في الفترة المخصّصة للصيانة فقط.

٥- ضبط إعدادات التحكّم بمعدل إرسال السجلات (Log Rate Limiting) لمنع تعرّض نظام التسجيل إلى هجمات حجب الخدمة، وضبط مستواه عند حد معقول.

٣-٢١ موارد تسجيل الأحداث (Logging Resources)

الهدف

تجنّب فقدان السجلات جرّاء استبدال البيانات المُخزّنة على وسائط التخزين.

المخاطر المحتملة

إن عدم التمكّن من توفير مساحة كافية لتخزين أقصى حدّ ممكن من السجلات قد يؤدي إلى استبدال المعلومات المُخزّنة في السجل وفقدان بيانات قيّمة ومهمّة خاصة بجامعة الملك فيصل. وفي هذه الحالة، من الممكن أن تُحذَف السجلات الحسّاسة بالكامل ولن تتمكّن جامعة الملك فيصل من الاعتماد على هذه السجلات في حال توجيه دعوى قضائية أو إجراء تحقيق معيّن، وهذا الأمر قد يؤثّر على أعمالها.

الإجراءات المطلوبة

١- توفير موارد كافية مثل موارد النظام، ووسائط تخزين البيانات، ونطاق الشبكة وذلك لاستيعاب أنشطة التسجيل المحدّدة.

٢- يجب أن تحتوي أجهزة تخزين السجلات على سعة تخزين كافية لجمع السجلات.

٣-٢٢ التغييرات على إعدادات التسجيل (Logging Configuration Changes)

الهدف

الحد من إمكانية إجراء أي تغييرات غير مصرّح بها أو ضارة على عملية تسجيل الأحداث الجاري تنفيذها في مكوّنات النظام.

المخاطر المحتملة

إذا لم تُفرَض أي قيود على المسؤول عن إدخال التغييرات على إعدادات السجل ومكان وموعد إجرائها، فإنه يُمكن أن يقوم مُستخدم خبيث بإيقاف التسجيل على الأجهزة الحسّاسة لتنفيذ هجوم غير ملحوظ.

الإجراءات المطلوبة

تقييد إمكانية تغيير إعدادات سجل الأحداث الأمنية، بما فيها نطاق العمل وآلية المراقبة، وحصرها على المستخدمين المصرّح لهم فقط.

٣-٢٣ استخدام أجهزة المراقبة (Use of Monitoring Devices)

الهدف

منع الكشف عن البيانات الحسّاسة والتأثير على شبكة الجامعة (مثل: استنزاف موارد الشبكة أو استخدام أدوات ضارة/خبيثة في البيئة).

المخاطر المحتملة

إذا لم تصرّح الإدارة المعنية بالأمن السيبراني في جامعة الملك فيصل ولم تسمح لموظفين معيّنين باستخدام أدوات أو أجهزة المراقبة والفحص، من الممكن أن تُستخدَم إحدى الأدوات بطريقة تضر البيئة وتزيد خطر انتهاك البيانات أو وقوع حادث أمني.

الإجراءات المطلوبة

١- تقييد استخدام أجهزة أو أدوات المراقبة والفحص على المستخدمين المصرّح لهم.

٢- تصنيف نتائج جميع أنشطة المراقبة والفحص ضمن المعلومات السريّة بحدٍّ أدنى.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٤. معيار الحماية من البرمجيات الضارة

الأهداف

الغرض من هذا المعيار هو تطبيق متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالحماية من البرمجيات الضارة في جامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية، وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل وينطبق هذا المعيار على جميع العاملين في جامعة الملك فيصل.

المعايير

٤-١ تطبيق تقنيات وآليات الحماية من البرمجيات الضارة (Malware Protection Solution (Implementation

الهدف

ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية لجامعة الملك فيصل، وذلك بتطبيق تقنيات وآليات للحماية من البرمجيات الضارة.

المخاطر المحتملة

يُعد غياب تقنيات وآليات الحماية من البرمجيات الضارة سبباً أساسياً في انتهاك سرية، أو سلامة، أو توافر البيانات، أو التطبيقات، أو نظم التشغيل نتيجة تسرب البرمجيات الضارة بمختلف أنواعها إلى أجهزة معالجة المعلومات الخاصة بجامعة الملك فيصل.

الإجراءات المطلوبة

١- يجب أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بالقدرات التالية:

- منع البرمجيات الضارة
- اكتشاف البرمجيات الضارة

٢- يجب أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بالقدرات اللازمة للحماية من مختلف أنواع البرمجيات الضارة ومنها:

- الفيروسات

- الديدان الحاسوبية
- فيروسات حصان طروادة
- برامج التجسس
- البرمجيات الضارة غير المعروفة مسبقًا

٣- يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة لحماية النهايات الطرفية في الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل بما في ذلك:

- جدار الحماية
- خوادم البريد الإلكتروني
- خوادم شبكة الويب
- الخوادم الوكيلة
- خوادم الوصول عن بُعد
- أجهزة المستخدمين
- الأجهزة المحمولة

٤- يجب أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بلوحة تحكم مركزية، مما يضمن التطبيق المتسق لسياسة الحماية من البرمجيات الضارة على جميع الأجهزة ومراقبة تهديدات هذه البرمجيات الضارة.

٥- يجب أن تتكون تقنيات وآليات الحماية من البرمجيات الضارة من واحدة أو أكثر من الأدوات التي تؤدي وظائف كل من:

- برامج مكافحة الفيروسات
- نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات
- جدار الحماية
- تصفية/فحص المحتوى
- السماح بقائمة محددة من التطبيقات

٦- يجب أن تُحدد وظائف تقنيات وآليات الحماية من البرمجيات الضارة بناءً على مخرجات عملية تقييم المخاطر.

٧- يجب إرسال سجلات الأحداث المتعلقة باكتشاف ومنع البرمجيات الضارة إلى تقنية الحماية من البرمجيات الضارة وإلى نظام سجلات الأحداث ومراقبة الأمن السيبراني لمراقبة الأحداث وتحليلها، وتحديد أوجه الارتباط، واتخاذ القرار.

٨- يجب الاستمرار على تطبيق آليات الحماية من البرمجيات الضارة للحد من أثر تهديدات البرمجيات الضارة في حال حدوثها. وتشمل هذه الآليات ما يلي:

- الحماية عبر إعدادات نظام الإدخال/الإخراج الأساسي (BIOS).
- آلية فصل التطبيقات غير الموثوقة.
- الفصل بين استخدامات المتصفح للتطبيقات المؤسسية وغير المؤسسية.
- الفصل من خلال الأنظمة الافتراضية.
- تقييد التفعيل التلقائي للملفات التي يتم تنزيلها أو البرامج المشتركة أو البرامج المجانية.

- اقتصار صلاحيات المستخدم النهائي على الجهاز الذي يستخدمه (دون منحه حقوق إدارية).
- تقييد التفعيل التلقائي أو استخدام الملفات المحتوية على حزم (Macros).
- حجب أنظمة التحميل والتشغيل (Booting Systems) الموجودة على الأقراص المرنة أو الأقراص المدمجة، إلا في الحالات الطارئة أو عند استخدام وسائط موثوقة.
- إعداد كافة البرمجيات لتنبيه المستخدم في حال فتح ملفات تحتوي على حزم (Macros).

٩- يجب أن يكون إجراء إزالة تثبيت برنامج تقنيات وآليات الحماية من البرمجيات الضارة محمياً بكلمة مرور وتتم إدارته عن بعد لضمان عدم قدرة المستخدم على إزالة تثبيت البرنامج أو تغيير إعداداته أو إلغاء تفعيله.

٢-٤ إعدادات تقنيات وآليات الحماية من البرمجيات الضارة (Malware Protection Solution Configuration)

الهدف

التأكد من تطبيق الإعدادات الصحيحة لتقنيات وآليات الحماية من البرمجيات الضارة وذلك لتوفير الحماية الفعالة من تهديدات البرمجيات الضارة.

المخاطر المحتملة

تؤدي الإعدادات غير المكتملة لتقنيات وآليات الحماية من البرمجيات الضارة إلى انتشار البرمجيات الضارة غير المكتشفة في بيئة جامعة الملك فيصل وبالتالي تقليل فعالية الحل بشكل عام.

الإجراءات المطلوبة

١- يجب ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة لإجراء فحص مباشر لجميع الملفات عند الوصول إليها أو نسخها أو نقلها لضمان اكتشاف جميع البرمجيات الضارة قبل تنشيطها.

٢- يجب إعداد برنامج تقنيات وآليات الحماية من البرمجيات الضارة لإجراء فحص كامل للنظام أسبوعياً على الأقل، ويمكن أن يكون وقت الفحص عند تشغيل النظام أو خلال ساعات الاستخدام المنخفض.

٣- تمكين خاصية فحص مكافحة البرمجيات الضارة للوسائط القابلة للإزالة عند إدخالها أو توصيلها.

٤- ضبط وإعداد الأجهزة بصورة تمنع التشغيل التلقائي للمحتوى.

٥- تفعيل خاصية تسجيل استعلامات نظام أسماء النطاقات (DNS) للكشف عن الاستعلامات الخاصة بنطاقات نظام أسماء النطاقات (DNS) الضارة المعروفة.

٦- تفعيل ميزات مكافحة الاستغلال على نظام التشغيل لاكتشاف و/أو منع الأنشطة المشبوهة والضارة.

٧- يجب ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة لاكتشاف البرمجيات الضارة أولاً ثم الاستجابة لها على النحو التالي: تصفية البرمجيات الضارة، أو حذفها، أو عزلها، أو تشفيرها. يجب أن يكون التشفير قابلاً للفك في حالة الاكتشاف الخاطئ لإحدى البرمجيات الضارة.

٨- ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة بحيث يقوم بعزل الملفات التي أصابها الفيروس في حال عدم القدرة على حذفها.

٩- ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة بحيث يقوم بتنبيه المستخدم بعدم قدرته على تنظيف أو عزل الشفرة الخبيثة.

١٠- تنصيب تقنيات وآليات الحماية من البرمجيات الضارة على خوادم البريد الإلكتروني، بما في ذلك بوابة بروتوكول إرسال البريد البسيط (SMTP). يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة بحيث تقوم بمسح محتوى الرسائل والمرفقات في كافة رسائل البريد الإلكتروني. وفي حال العثور على برمجيات ضارة في بروتوكول إرسال البريد البسيط (SMTP) الوارد، يجب اتباع الإجراءات التالية:

- حذف الفيروسات بالمرفقات المصابة.
- عزل المرفقات المصابة في حال عدم القدرة على مسحها.

١١- ضبط إعدادات نظام التشغيل والتطبيقات على لوحة التحكم المركزية بتقنيات وآليات الحماية من البرمجيات الضارة وفقاً لإرشادات الإعداد الآمن التي يوفرها المورد.

١٢- منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت والمعروفة باستضافتها لمحتوى خبيث باستخدام آلية تصفية محتوى الويب.

١٣- تقوم جامعة الملك فيصل بمراقبة الأداء للمعايير التالية:

- استخدام وحدة التحكم المركزية (CPU)
- استخدام الذاكرة
- أداء الشبكة
- استخدام القرص

١٤- يجب أن يقدم مشرفو تقنيات وآليات الحماية من البرمجيات الضارة تقاريراً شهرية حول حالة الحماية من البرمجيات الضارة إلى إدارة الأمن السيبراني في جامعة الملك فيصل. ويجب أن يتضمن التقرير على الأقل ما يلي:

- عدد أجهزة الحاسوب والخوادم وأجهزة الحاسوب المحمولة والأنظمة غير المحدثة بأحدث أنماط التواقيع.
- أهم ١٠ برمجيات ضارة تم اكتشافها.
- عدد الفيروسات/الديدان الحاسوبية/البرامج الخبيثة المكتشفة.
- عدد الفيروسات/الديدان الحاسوبية/البرامج الخبيثة التي تم تنظيفها/عزلها/حذفها.
- الإجراء المُتخذ لحل مشكلة الإصابة بالبرمجيات الضارة.
- مصدر الإصابة.

٤-٣ تحديثات تقنيات وآليات الحماية من البرمجيات الضارة (Malware Protection Solution Updates)

الهدف

ضمان تحديث تقنيات وآليات الحماية من البرمجيات الضارة لحماية الأصول المعلوماتية والتقنية من أحدث البرمجيات الضارة المعروفة.

المخاطر المحتملة

يمكن أن تمر أحدث البرمجيات الضارة المعروفة دون أن يتم كشفها، وقد تؤدي إلى انتهاك الأمن السيبراني لجامعة الملك فيصل في حال عدم تحديث تقنيات وآليات الحماية من البرمجيات الضارة بأحدث التواقيع.

الإجراءات المطلوبة

١- يجب تحديث تقنيات وآليات الحماية من البرمجيات الضارة بشكل مستمر وتلقائي وفقاً لسياسة إدارة التحديثات والإصلاحات.

٢- يجب التحقق من سلامة المعلومات والملفات الخاصة بتقنيات وآليات الحماية من البرمجيات الضارة دورياً.

٣- يجب تحديث قاعدة بيانات تواقيع تقنيات وآليات الحماية من البرمجيات الضارة تلقائياً أو يدوياً بشكل منتظم.

٤- يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة للحصول على نمط التواقيع من الموقع الإلكتروني للمورد.

٥- يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة "لتوزيع" آخر تحديثات التواقيع على أجهزة المستخدمين والخوادم.

٦- يجب ضبط إعدادات الأجهزة غير الموجودة ضمن شبكة الأجهزة المحمولة في جامعة الملك فيصل لتتضمن خيارات تحديث بديلة بحيث يمكن تحديث التواقيع مباشرة من الموقع الإلكتروني للمورد.

٧- يجب أن تدعم تقنيات وآليات الحماية من البرمجيات الضارة استرجاع تحديثات التواقيع في حال أدت آخر التحديثات إلى عدم اتساق برنامج مكافحة الفيروسات وأثرت على قدرته على العمل بالصورة المتوقعة.

٤-٤ تتبع التهديدات والثغرات الجديدة (Tracking New Threats and Vulnerabilities)

الهدف

التحديد المبكر للتهديدات الجديدة التي يمكن أن تؤثر على أمن جامعة الملك فيصل وضمان اتخاذ الإجراءات المناسبة للحد من المخاطر المرافقة.

المخاطر المحتملة

يمكن أن تتعرض جامعة الملك فيصل لانتهاك أمني نتيجة عدم القدرة على كشف البرمجيات الضارة الخبيثة الجديدة وغير المعروفة.

الإجراءات المطلوبة

١- يجب أن تتابع جامعة الملك فيصل التهديدات الجديدة الناشئة عن الشفرات الخبيثة ويجب أن تحتفظ بقائمة بكافة السيناريوهات المحتملة للإصابة بالبرمجيات الخبيثة (مثل: كيف يمكن للفيروس أن يؤثر على الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل وما هي طريقة وصوله إليها).

٢- يجب تحديد السيناريوهات بوضوح ويجب أن تتصدى تقنيات الحماية من البرمجيات الضارة لهذه البرمجيات وتتخلص منها على كافة المستويات.

٣- عند وجود ثغرات جديدة، يجب أن تحدد جامعة الملك فيصل الخطوات التي يجب اتخاذها لضمان الحد من المخاطر المحتملة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني** .
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني**.
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني** وإدارة الأمن السيبراني.

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٥. معيار أمن أجهزة المستخدمين

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة أجهزة المستخدمين والأجهزة المحمولة (Workstation) الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة عن الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أجهزة المستخدمين المكتبية والمحمولة الخاصة بجامعة الملك فيصل، وينطبق على جميع العاملين في جامعة الملك فيصل.

المعايير

٥-١ الوصول الآمن (Secure Access)

الهدف

ضمان حماية أجهزة المستخدمين ووظائفها من الوصول غير المصرح به.

المخاطر المحتملة

ينطوي على الوصول غير المصرّح به إلى أجهزة المستخدمين مخاطر كبيرة قد تؤدي إلى سرقة المعلومات ووقوع انتهاكات أمنية تُمكن منفذيها من شن المزيد من الهجمات الضارة ضد موظفي جامعة الملك فيصل وبنيتها التحتية أو ضد أي هدف خارجي آخر.

الإجراءات المطلوبة

١- تقييد الوصول إلى أجهزة المستخدمين وحصره على حساب المستخدم للجهاز.

٢- تطبيق مبدأ الحد الأدنى من الصلاحيات والامتيازات عند منح الصلاحيات على أجهزة المستخدمين.

٣- إلغاء أو إعادة تسمية الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة.

٤- إلى جانب استخدام تركيبة اسم المستخدم/كلمة المرور، إلزام المستخدم باستخدام آليات المصادقة أو التحقّق من الهوية متعدّد العناصر (MFA)، مثل الخصائص الحيوية والمفاتيح المادية وكلمات المرور المؤقتة والبطاقات الذكية وشهادات التشفير وغيرها، على أجهزة المستخدمين في البيئات فائقة الحماية مثل مركز العمليات الأمنية (SOC).

٥- إعداد متطلبات تعقيد كلمة المرور الخاصة بجهاز المستخدم وفقاً لسياسة إدارة هويات الدخول والصلاحيات في جامعة الملك فيصل.

٦- ضبط وإعداد حد الإغلاق بعد عدد معين من محاولات تسجيل الدخول غير الناجحة وانتهاء وقت الجلسة وتسجيل الخروج في حال عدم الاستخدام بالنسبة لحالات الوصول المحلية والوصول إلى النطاقات وفقاً لسياسة إدارة هويات الدخول والصلاحيات في جامعة الملك فيصل.

٧- ضبط وإعداد كلمات مرور مُحمِّل التشغيل (Bootloader) لنظام الإدخال/الإخراج الأساسي (BIOS).

٢-٥ مراجعة الإعدادات والتحصين (Secure Hardening Configuration)

الهدف

تحديد متطلبات الأمن الأساسية لأجهزة المستخدمين لضمان تصميم أجهزة المستخدمين وإعدادها وتشغيلها بطريقة آمنة.

المخاطر المحتملة

يمكن أن يؤدي الإعداد الخاطئ والتصميم غير الآمن لأجهزة المستخدمين إلى ثغرات أمنية يمكن استغلالها لتهديد سرية وسلامة وتوافر بيانات جامعة الملك فيصل وسير عملها.

الإجراءات المطلوبة

١- إجراء اختبارات أمنية منتظمة (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في جامعة الملك فيصل.

٢- إجراء التحديثات والإصلاحات على أجهزة المستخدمين بانتظام وفقاً لسياسة أمن أجهزة المستخدمين وسياسة إدارة التحديثات والإصلاحات في جامعة الملك فيصل لضمان تحديث جميع أنظمة التشغيل وبرمجيات التطبيقات على أجهزة المستخدمين.

٣- حذف التطبيقات والخدمات غير الضرورية أو غير اللازمة أو إلغاء تفعيلها على أجهزة المستخدمين مثل بروتوكول تل نت (Telnet)، ولوحة المفاتيح باللمس، والسجل عن بعد (إذا لم يكن ضرورياً)، وغيرها.

٤- حذف/تعطيل خصائص نظام التشغيل والتطبيق وملفات الإعدادات غير الضرورية أو غير اللازمة أو إلغاء تفعيلها.

٥- حجب إمكانية الوصول إلى أدلة الشبكة والملفات غير الضرورية أو غير اللازمة.

٦- استخدام الضوابط المادية وحظر الوصول إلى الوسائط القابلة للإزالة عند الضرورة أو وفقاً لسياسة الاستخدام المقبول في جامعة الملك فيصل.

٧- تطبيق الإعدادات والتحصين لأجهزة المستخدمين بما في ذلك التحصين على مستوى البرمجيات وأنظمة التشغيل وفقاً لسياسة الإعدادات والتحصين في جامعة الملك فيصل.

٨- إنشاء نسخ وقوالب آمنة لأجهزة المستخدمين بناءً على معايير الإعدادات المعتمدة ووفقاً لسياسة الإعدادات والتحصين في جامعة الملك فيصل. وإعادة نسخ الأجهزة باستخدام أحد قوالب نسخ أجهزة المستخدمين في حال تعرضها لانتهاك أمني.

٩- تخزين نسخ أجهزة المستخدمين في بيئة آمنة على نسخ احتياطية أو بيئة تخزين معدة بصورة آمنة وغير مرتبطة بالشبكة والتحقق بانتظام من هذه النسخ باستخدام أدوات مراقبة سلامة المعلومات.

٥-٣ النسخ الاحتياطي والأرشفة (Backup and Archiving)

الهدف

ضمان سلامة بيانات أجهزة المستخدمين من العبث بها أو فقدانها بالخطأ أو تخريبها والتأكد من توافرها وإمكانية استعادتها.

المخاطر المحتملة

في حال حذف بيانات أجهزة المستخدمين بالخطأ أو العبث بها أو فقدانها أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن جامعة الملك فيصل من استعادة البيانات، مما سيؤثّر في أنشطة أعمالها الاعتيادية.

الإجراءات المطلوبة

١- عمل نسخ احتياطية كاملة وتزايدية لأجهزة المستخدمين وفقاً لسياسة إدارة النسخ الاحتياطي المعتمدة في جامعة الملك فيصل. ويجب أن تشمل النسخ الاحتياطية على الأقل نسخاً احتياطية لنظام تشغيل أجهزة المستخدمين، ونسخاً احتياطية لإعدادات البرمجيات، ونسخاً احتياطية للبيانات.

٢- تخزين النسخ الاحتياطية لثلاث فترات متتالية بما في ذلك الفترة الحالية. فعلى سبيل المثال، إذا تم عمل النسخ الاحتياطية شهرياً، يجب تخزين النسخ الاحتياطية للشهر الحالي ولشهرين سابقين فقط.

٣- تشفير النسخ الاحتياطية لأجهزة المستخدمين الخاصة بجامعة الملك فيصل.

٤- ترتيب النسخ الاحتياطية الخاصة بأجهزة مستخدمي جامعة الملك فيصل تسلسلياً وتسجيل وقتها، وتاريخها، وجدولتها.

٥- اختبار إمكانية استرجاع النسخة الاحتياطية كل ثلاثة أشهر وفقاً لسياسة إدارة النسخ الاحتياطي المعتمدة في جامعة الملك فيصل.

٦- تطبيق آليات توثيق النسخ الاحتياطي وسلامتها لضمان نسخ بيانات أجهزة المستخدمين أو أرشفتها بطريقة صحيحة.

٥-٤ برمجيات حماية الأجهزة الطرفية (Endpoint Protection Software)

الهدف

ضمان حماية أجهزة المستخدمين من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقاً وأي نوع آخر من الهجمات الخبيثة.

المخاطر المحتملة

يمكن أن تؤدي الهجمات الخبيثة الناجحة على أجهزة المستخدمين إلى تعريض جامعة الملك فيصل لاختراق أمني أو الوصول غير المصرح به أو الكشف عن بياناتها في حال تركت أجهزة المستخدمين دون حماية.

الإجراءات المطلوبة

١- ضبط وإعداد حد إغلاق نظام التشغيل ووظائف التطبيقات عن طريق الحد الأدنى من الصلاحيات والامتيازات المطلوبة للتشغيل في الظروف الاعتيادية، مثل إلغاء تفعيل تغيير وقت النظام يدوياً، وتعديل ملفات النظام، وإنشاء الملفات أو تعديلها أو حذفها، وغيره.

٢- تطبيق خاصية السماح بقائمة محددة من التطبيقات على أجهزة المستخدمين لتمكين عمل تطبيقات وبرمجيات محددة فقط وفقاً للحاجة.

٣- تطبيق خاصية السماح بقائمة محددة من التطبيقات لاستخدام خاصيتين لتحديد التطبيق، بما في ذلك على سبيل المثال وليس الحصر، قواعد التجزئة المشفرة أو قواعد شهادات الناشر أو قواعد المسار للسماح باستخدام التطبيقات أو منعها.

٤- ضبط إعدادات أنظمة السماح بقائمة محددة من التطبيقات بحيث لا يمكن للمستخدمين إلغاء تفعيل الأنظمة باستثناء المديرين عند أدائهم لمهام إدارية معينة تقتضي إلغاء تفعيل السماح بقائمة محددة من التطبيقات مؤقتاً.

٥- فيما يخص خاصية السماح بقائمة محددة من التطبيقات، يجب تعريف الملفات التنفيذية المعتمدة (exe, com, pif، وغيرها) ومكتبات البرمجيات (dll, ocx، وغيرها) والنصوص (ps1, bat, vbs، وغيرها) وبرامج التثبيت (msi, msp، وغيرها) من أجل تنفيذ الملفات من القائمة المعتمدة فقط.

٦- تطبيق نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Prevention System "HIPS") على جميع أجهزة المستخدمين.

٧- تطبيق جدار حماية من البرمجيات المستضافة على جميع أجهزة المستخدمين.

٨- تطبيق برامج مكافحة الفيروسات على جميع أجهزة المستخدمين.

٩- تطبيق برامج مكافحة البرامج الضارة على جميع أجهزة المستخدمين.

١٠- تطبيق برامج الحماية من التهديدات المتقدمة المستمرة (APT) على جميع أجهزة المستخدمين.

١١- تطبيق برامج اكتشاف أجهزة النهاية الطرفية والاستجابة لها على جميع أجهزة المستخدمين.

١٢- تطبيق برمجيات التحكم بأجهزة النهاية الطرفية على كافة أجهزة المستخدمين لمنع أي دخول من أجهزة خارجية غير مصرحة.

٥-٥ تسجيل الأحداث وسجل التدقيق (Event and Audit Logging)

الهدف

التأكّد من توثيق وتسجيل الأحداث الأمنية والأنشطة غير المصرّح بها التي تشهدها أجهزة المستخدمين.

المخاطر المحتملة

قد يؤدي عدم تفعيل وتسجيل الأحداث الأساسية التي تُنفذ في أجهزة المستخدمين والتي حدّدتها متطلّبات الضابط إلى صعوبة اكتشاف ومنع الهجمات السيبرانية، أو إساءة استخدام الصلاحيات الهامة والحساسة، مما قد يؤثّر على أعمال جامعة الملك فيصل.

الإجراءات المطلوبة

١- ضبط وإعداد سجل أجهزة المستخدمين وسجل التدقيق ليتم ترحيلهما إلى نظام تسجيل مركزي وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني في جامعة الملك فيصل.

٢- إعداد أجهزة المستخدمين ليتزامن توقيتها مع توقيت ثلاثة أجهزة تزامن مركزية على الأقل مما يسمح بتزامن توقيت سجلات الأحداث.

٣- ضبط إعدادات أجهزة المستخدمين وذلك بحفظ سجلات الأحداث المحلية، وسجلات التدقيق والسجلات الأمنية، بحيث تشمل جميع مستويات السجلات.

٥-٦ التشفير (Cryptography)

الهدف

ضمان الحفاظ على سريّة بيانات المستخدمين والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.

المخاطر المحتملة

قد يؤدي عدم وجود التقنيات الأمنية المناسبة لضمان تشفير بيانات أجهزة المستخدمين إلى تعرض بيانات جامعة الملك فيصل لمخاطر سيبرانية عالية نتيجة الوصول غير المصرح به إلى هذه البيانات.

الإجراءات المطلوبة

١- تطبيق تقنيات التشفير مثل أمن طبقة النقل (TLS) والشبكات الخاصة الافتراضية (VPN) لحماية آليات التحقّق من الهوية أثناء إرسال الرسائل، واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) الموصي بها. للمزيد من التفاصيل، يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة الملك فيصل.

٢- تشفير وسائط التخزين في أجهزة المستخدمين بما في ذلك الأقراص الصلبة حيثما كان ذلك ضرورياً وفقاً للسياسات والإجراءات ذات العلاقة في جامعة الملك فيصل.

٣- استخدام بروتوكول إدارة أجهزة المستخدمين الذي يدعم التشفير أو يقوم بضبط إعدادات التشفير لبروتوكولات إدارة أجهزة المستخدمين مثل: بروتوكول النفاذ إلى الدليل البسيط (LDAP) على أمن طبقة النقل (TLS)، والنسخة الثالثة من بروتوكول إدارة الشبكة البسيط (SNMPv3) لغايات المصادقة والخصوصية، وبروتوكول كيربيروس (Kerberos) مع أمن طبقة النقل (TLS)، وسجل النظام المشفر، وغيرها.

٥-٧ الإدارة المركزية (Central Management)

الهدف

تحديد المتطلبات الأمنية لإدارة أجهزة المستخدمين لضمان تشغيل أجهزة المستخدمين وإداراتها مركزياً وبطريقة آمنة وضمان تطبيق جميع المتطلبات الأمنية وتنفيذها.

المخاطر المحتملة

يؤدي الافتقار إلى الإدارة الآمنة وعدم تطبيق المتطلبات الأمنية على أجهزة المستخدمين إلى زيادة احتمالية التعرض للهجمات، ويزيد من فرص وجود ثغرات ونقاط ضعف في بيئة جامعة الملك فيصل يمكن استغلالها في الهجمات أو الاختراقات الخبيثة، مما يعرض أجهزة المستخدمين والبيانات في جامعة الملك فيصل إلى انتهاكات أمنية.

الإجراءات المطلوبة

١- ضبط إعدادات خادم الإدارة المركزية أو خادم النطاق ليطبق سياسة أمن الخوادم في جامعة الملك فيصل على جميع أجهزة المستخدمين.

٢- تثبيت أدوات إدارة إعدادات النظام التي تنفذ إعدادات الضبط والتهيئة لأجهزة المستخدمين وتعيد تثبيتها تلقائياً في فترات زمنية محددة ومنتظمة. للمزيد من التفاصيل، يرجى الرجوع إلى سياسة الإعدادات والتحصين في جامعة الملك فيصل.

٣- تطبيق نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة محتوى الأمن ("SCAP" Security Content Automation Protocol) للتأكد من عناصر الإعدادات الأمنية كافة وجدولة الاستثناءات المعتمدة والإبلاغ عن حدوث أي تغييرات غير مصرّح بها.

٨-٥ أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (Privileged Access Workstations "PAW")

الهدف

تحديد المتطلبات الأمنية الإضافية لحماية أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs) المستخدمة في الوصول إلى الأنظمة ومناطق الشبكة الهامة.

المخاطر المحتملة

يمكن أن تؤدي الهجمات الخبيثة الناجحة على أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة إلى تعريض جامعة الملك فيصل لاختراقات خطيرة وانتهاكات أمنية لأهم أصولها الحساسة مما يؤدي إلى أضرار جسيمة.

الإجراءات المطلوبة

١- فرض استخدام التحقّق من الهوية متعدّد العناصر من أجل الوصول إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) التي يستخدمها مديرو النظام.

٢- تقييد الوصول إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) وحصره على المشرفين والمشغلين المصرح لهم فقط.

٣- وضع أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) في منطقة الإدارة في الشبكة.

٤- تشفير جميع أنواع الحركة المنقولة من أو إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) بما في ذلك حركة الوصول الإداري والتحكم (مثل بروتوكول النقل الآمن "SSH"، وبروتوكول التحكم بسطح المكتب عن بعد "RDP")، وحركة البيانات باستخدام آليات التشفير (مثل أمن طبقة النقل "TLS") وفقاً لمعيار التشفير المعتمد في جامعة الملك فيصل.

٥- إلغاء تفعيل خاصية الوصول إلى الإنترنت على أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW).

٦- إلغاء تفعيل الخدمات الخطرة وغير اللازمة (مثل إرسال رسائل البريد الإلكتروني واستلامها) على أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW).

٧- تفعيل جميع مستويات التسجيل، إلى جانب سجل التدقيق والسجلات الأمنية، محلياً وعلى نظام تسجيل أحداث مركزي.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.

قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٦. معيار أمن الخوادم

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة الخوادم الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الخوادم الخاصة بجامعة الملك فيصل، وينطبق على جميع العاملين في جامعة الملك فيصل.

المعايير

٦-١ الوصول الآمن (Secure Access)

الهدف

ضمان حماية الخوادم ووظائفها من الوصول غير المصرح به.

المخاطر المحتملة

ينطوي الوصول غير المصرّح به إلى الخوادم على مخاطر عالية قد تؤدي إلى تسريب البيانات، أو سرقتها، أو تعطيل الخدمات، أو انتهاكات أمنية تسمح لمنفذيها باستخدامها لشن المزيد من الهجمات السيبرانية ضد جامعة الملك فيصل وبنيتها التحتية.

الإجراءات المطلوبة

١- استخدام مبدأ الحماية الذي يمنح مشرفي ومُشغّلي الخوادم الحد الأدنى من صلاحيات الوصول إلى مختلف أنواع أنظمة البريد الإلكتروني.

٢- حصر الوصول إلى الخوادم على مشرفي الخوادم فقط وذلك من خلال منح حق الوصول لحسابات المشرفين المختلفين وبروتوكول الإنترنت لأجهزة المستخدمين باستخدام قوائم التحكم بالوصول (ACLs).

٣- إيقاف، أو تغيير الحسابات الافتراضية، أو غير التفاعلية، أو غير اللازمة.

٤- إلى جانب ضرورة إدخال اسم المستخدم وكلمة المرور، إلزام المستخدم باستعمال آليات أخرى للتحقّق من الهوية مثل السمات الحيوية، والمفاتيح المادية، وكلمات المرور المؤقتة، والبطاقات الذكية، وشهادات التشفير، وغيرها.

٥- إعداد متطلبات تعقيد كلمة المرور الخاصة بالخادم وفقاً لسياسة إدارة هويات الدخول والصلاحيات في جامعة الملك فيصل.

٦- تطبيق تقنيات التشفير مثل «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية آليات التحقّق من الهوية أثناء إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) الموصي بها. للمزيد من التفاصيل، يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة الملك فيصل.

٧- تطبيق نظام إدارة الصلاحيات الهامة والحسّاسة (PAM) لمنح حق الوصول المؤقت إلى الخوادم القائم على نوع الجلسة المطلوبة.

٨- ضبط وإعداد وقت انتهاء الجلسة وحد إغلاق الجلسة عند عدم الاستخدام وفقاً لسياسات الأمن السيبراني في جامعة الملك فيصل.

٩- ضبط وإعداد كلمات مرور مُحمِّل تشغيل (Bootloader) نظام الإدخال/الإخراج الأساسي (BIOS).

١٠- إلزام مشرفي ومُشغّلي الخوادم باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى الخوادم الحساسة.

١١- تقييد وصول المشرفين والمشغلين إلى الخوادم الحساسة وحصره على أجهزة الحاسب ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs).

١٢- تقييد الوصول إلى الخوادم وحصره على المشرفين والمشغلين وذلك عن طريق خوادم الوصول إلى المناطق الآمنة (Jump Servers) أو إدارة الصلاحيات الهامة والحسّاسة (PAM).

- استخدام خوادم منفصلة للوصول إلى المناطق الآمنة (Jump Servers) لمشرفي ومستخدمي النظام.
- استخدام التحقّق من الهوية متعدّد العناصر من أجل الوصول عبر خوادم الوصول إلى المناطق الآمنة (Jump Server) المستخدمة من قبل مشرفي النظام وذلك من خلال تطبيق قوائم التحكم بالوصول (ACLs).
- تقييد الوصول إلى خوادم الوصول إلى المناطق الآمنة (Jump Servers) وحصره على المشرفين والمشغلين المصرح لهم فقط.
- تقييد الوصول إلى الشبكة وحصره على خوادم الوصول إلى المناطق الآمنة (Jump Servers) من خلال تطبيق قوائم التحكم بالوصول (ACLs).
- وضع خوادم الوصول إلى المناطق الآمنة (Jump Servers) في منطقة إدارة الشبكة.
- إلغاء تفعيل خاصية الوصول إلى الإنترنت على خوادم الوصول إلى المناطق الآمنة (Jump Servers).
- إلغاء تفعيل الخدمات الخطرة وغير اللازمة (مثل إرسال رسائل البريد الإلكتروني واستلامها) على خوادم الوصول إلى المناطق الآمنة (Servers Jump).
- تفعيل جميع مستويات التسجيل إضافةً إلى سجل التدقيق والسجلات الأمنية محلياً وعلى نظام تسجيل أحداث مركزي.

٢-٦ مراجعة الإعدادات والتحصين (Secure Hardening Configuration)

الهدف

تحديد متطلبات الأمن الأساسية للخوادم لضمان تصميم الخوادم وإعدادها وتشغيلها بطريقة آمنة.

المخاطر المحتملة

يعتبر الإعداد الخاطئ للخوادم والتصميم الضعيف من الثغرات الأمنية الشائعة التي يمكن استغلالها لتهديد سرية وسلامة وتوافر بيانات جامعة الملك فيصل وسير عملها.

الإجراءات المطلوبة

١- إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في جامعة الملك فيصل.

٢- إجراء التحديثات والإصلاحات على الخوادم بانتظام وفقاً لسياسة إدارة التحديثات والإصلاحات في جامعة الملك فيصل لضمان تحديث جميع أنظمة التشغيل وبرمجيات التطبيقات على الخوادم.

٣- حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من الخوادم مثل خدمات الطباعة، وبروتوكول تل نت (telnet)، وغيره.

٤- استخدام مبدأ الحماية الذي يمنح مشرفي ومُشغّلي الخوادم الحد الأدنى من صلاحيات الوصول إلى مختلف أنواع الأنظمة.

٥- حصر الوصول إلى الشبكة بمناطق الخوادم ومناطق إدارة الخوادم.

٦- حذف أو إلغاء تفعيل خصائص نظام التشغيل والتطبيق وملفات الإعدادات غير الضرورية أو غير اللازمة.

٧- حجب إمكانية الوصول إلى مجلدات الشبكة والملفات غير الضرورية أو غير اللازمة.

٨- استخدام ضوابط الأجهزة وحجب الوصول إلى وسائط التخزين القابلة للإزالة.

٩- إنشاء البنية التحتية للخوادم تبعاً لبنية متعدّدة الطبقات محمية باستخدام جدران حماية ذات طبقة مزدوجة. وإدراج خادم ويب في منطقة الإنترنت المحايدة، وخوادم التطبيقات في منطقة الإنتاج، وخوادم قواعد البيانات في المنطقة الموثوقة أو منطقة قاعدة البيانات.

١٠- العزل المادي أو المنطقي لخوادم الأنظمة الحساسة عن الخوادم أو الأنظمة الأخرى. فعلى سبيل المثال، يمكن تحقيق العزل المادي من خلال استضافة الخوادم في بيئة مادية منفصلة ومختلفة تماماً، ويمكن تحقيق العزل المنطقي من خلال تطبيق الخوادم في مناطق منفصلة داخل الشبكة دون السماح بالوصول إليها من أي منطقة أخرى.

١١- ضبط إعدادات وتحصين الخوادم بما في ذلك التحصين على مستوى التطبيقات وقاعدة البيانات ونظام التشغيل.

١٢- إنشاء نسخ أو قوالب آمنة لكافة الخوادم بناءً على معايير الإعدادات المعتمدة، وإعادة نسخ الخوادم باستخدام أحد قوالب نسخ الخوادم في حال تعرضها لانتهاك أمني.

١٣- تخزين نسخ الخوادم في بيئة آمنة على خوادم معدة بصورة آمنة والتحقق بانتظام من هذه النسخ باستخدام أدوات مراقبة سلامة المعلومات.

١٤- تطبيق الفصل المنطقي أو المادي للخوادم بين بيئات الإنتاج والتطوير والاختبار.

٦-٣ النسخ الاحتياطي والأرشفة (Backup and Archiving)

الهدف

ضمان سلامة بيانات الخوادم وتوافرها وقابلية استعادتها والتأكد من عدم العبث بها أو فقدانها بالخطأ أو تخريبها.

المخاطر المحتملة

في حال حذف بيانات الخوادم أو فقدانها بالخطأ أو العبث بها أو تخريبها أو تعرّضها إلى هجوم إلكتروني، لن تتمكّن جامعة الملك فيصل من استرداد البيانات مما سيؤثّر على أنشطة أعمالها الاعتيادية.

الإجراءات المطلوبة

١- عمل نسخة احتياطية كاملة للخوادم وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة الملك فيصل. يجب أن تشمل النسخ الاحتياطية على الأقل نسخاً احتياطية لنظام تشغيل الخوادم، ونسخاً احتياطية لإعدادات التطبيقات، ونسخاً احتياطية لإعدادات قواعد البيانات، وقواعد البيانات والمعلومات المخزنة.

٢- يجب تشفير النسخ الاحتياطية للخوادم وكذلك فك التشفير في حالة عمل استرداد للبيانات الموجودة بإصدار النسخة الاحتياطية.

٣- إضافة ترتيب تسلسلي للنسخ الاحتياطية عن الخوادم الخاصة بجامعة الملك فيصل وتسجيل وقتها وتاريخها وجدولتها.

٤- تخزين النسخ الاحتياطية عن الخوادم الخاصة بجامعة الملك فيصل في موقعين خارجيين محميّين منفصلين على الأقل.

٥- اختبار إمكانية استرجاع النسخة الاحتياطية كل ثلاثة أشهر وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة الملك فيصل.

٦- تطبيق آليات توثيق النسخ الاحتياطية وسلامتها لضمان نسخ بيانات أجهزة المستخدمين أو أرشفتها بطريقة صحيحة.

٧- أرشفة النسخ الاحتياطية لخوادم جامعة الملك فيصل في موقع تخزين غير مرتبط بالشبكة طوال فترة التخزين المعتمدة وفقاً لسياسة إدارة النسخ الاحتياطية في جامعة الملك فيصل.

٤-٦ حماية الخوادم (Server Protection)

الهدف

ضمان حماية الخوادم من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقاً وأي نوع آخر من الهجمات الخبيثة.

المخاطر المحتملة

يمكن أن تؤدي الهجمات الخبيثة الناجحة على الخوادم إلى تعريض جامعة الملك فيصل لاختراق أمني أو وصول غير مصرح به أو الكشف عن البيانات في حال تركت الخوادم دون حماية.

الإجراءات المطلوبة

١- ضبط وإعداد حد إغلاق نظام التشغيل ووظائف التطبيقات عن طريق الحد الأدنى من الصلاحيات والامتيازات المطلوب للتشغيل في الظروف الاعتيادية، مثل إلغاء تفعيل تغيير وقت النظام يدوياً، والإغلاق/إعادة التشغيل، وتعديل ملفات النظام، وإنشاء/تعديل/حذف الملفات، وغيرها.

٢- تطبيق خاصية السماح بقائمة محددة من التطبيقات على الخوادم لتمكين عمل تطبيقات وبرمجيات محددة فقط وفقاً للحاجة.

٣- إعداد أنظمة السماح بقائمة محددة من التطبيقات بحيث لا يمكن للمستخدمين إلغاء تفعيل الأنظمة باستثناء مديري النظام عند أدائهم لمهام إدارية معينة تقتضي إلغاء تفعيل السماح بقائمة محددة من التطبيقات مؤقتاً.

٤- تعريف الملفات التنفيذية المعتمدة (exe, com, pif، وغيرها) ومكتبات البرمجياتocx (,dll، وغيرها) والنصوص (ps1, bat, vbs، وغيرها) وبرامج التثبيت (msi, msp، وغيرها).

٥- تطبيق خاصية السماح بقائمة محددة من التطبيقات لاستخدام قواعد التجزئة المشفرة أو قواعد شهادات الناشر أو قواعد المسار للسماح باستخدام التطبيقات أو منعها.

٦- ضبط وإعداد مجلدات التطبيقات وفقاً لتصاريح نظام الملفات لمنع أي تعديل غير مصرح به على المجلد أو تصاريح الملفات.

٧- تمكين وظيفة الحماية على الخوادم لاستخدامها في إجراءات الحد من المخاطر على نظام التشغيل وإجراءات الحد من المخاطر لتطبيقات معينة.

٨- تطبيق نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيفمعيارف (Intrusion Prevention System Host-based "HIPS") على جميع الخوادم.

٩- تطبيق جدار حماية من البرمجيات المستضافة على جميع الخوادم.

١٠- تطبيق برامج مكافحة الفيروسات على جميع الخوادم.

١١- تطبيق حماية النهاية الطرفية (Endpoint Protection) على جميع الخوادم.

١٢- تطبيق برامج الحماية من التهديدات المتقدمة المستمرة (APT) على جميع الخوادم.

١٣- تطبيق برمجيات التحكم بأجهزة النهاية الطرفية على كافة الخوادم لمنع الاستخدام غير المصرح به للأجهزة.

١٤- تطبيق جميع المتطلبات بموجب سياسة الحماية من البرمجيات الضارة المعتمدة في جامعة الملك فيصل.

٥-٦ تسجيل الأحداث وسجل التدقيق (Event and Audit Logging)

الهدف

ضمان الحفاظ على سريّة بيانات الخوادم والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.

المخاطر المحتملة

عدم إمكانية التأكّد من سلامة البيانات وموثوقيتها على الخوادم، مما قد يؤثر على حماية جامعة الملك فيصل من الهجمات الخبيثة والكشف عن المعلومات المهمّة والحسّاسة والوصول غير المصرّح به.

الإجراءات المطلوبة

١- ضبط وإعداد سجل الخوادم وسجل التدقيق ليتم ترحيلها إلى نظام تسجيل مركزي وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني في جامعة الملك فيصل.

٢- إعداد الخوادم ليتزامن وقتها مع ثلاثة خوادم زمنية إضافية على الأقل في غضون أجزاء من الثانية بطريقة ممكنة تقنياً مما يسمح باتساق الأختام الزمنية في السجلات.

٣- ضبط إعدادات الخوادم ذات الخطورة العالية التي تعتمد عادةً على التسجيل المركزي لحفظ سجلات أنظمة التشغيل في حال تعطّل اتصال الشبكة.

٦-٦ التشفير (Cryptography)

الهدف

ضمان الحفاظ على سريّة بيانات الخوادم والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.

المخاطر المحتملة

عدم إمكانية تشفير بيانات الخوادم والتأكّد من سلامة تلك البيانات وموثوقيتها وحمايتها، مما قد يؤثر على الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة الخاصة بالجامعة.

الإجراءات المطلوبة

١- تطبيق تقنيات التشفير مثل «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية آليات التحقّق من الهوية أثناء إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) الموصي بها. لمزيد من التفاصيل، يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة الملك فيصل.

٢- تشفير وسائط التخزين في الخوادم بما في ذلك الأقراص الصلبة، ووسائط التخزين الملحقة بالشبكة (NAS)، ووسائط التخزين المتصلة بشبكة التخزين (SAN)، أو أي نوع آخر من وسائط التخزين المتصلة.

٣- استخدام بروتوكول إدارة الخوادم الذي يدعم التشفير أو يقوم بضبط إعدادات التشفير لبروتوكولات إدارة الخوادم، مثل بروتوكول النفاذ إلى الدليل البسيط (LDAP) على أمن طبقة النقل (TLS)، والنسخة الثالثة من بروتوكول إدارة الشبكة البسيط (SNMPv3) لغايات المصادقة والخصوصية، وبروتوكول كيربيروس (Kerberos) مع أمن طبقة النقل (TLS)، وسجل النظام المشفر، وغيرها.

٤- إعداد التشفير لتطبيقات الخوادم وبروتوكولات الاتصال بقواعد البيانات، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS)، وواجهة برمجة التطبيقات الآمنة (API)، وتشفير البيانات الشفاف (TDE)، أو برنامج (SQL) على أمن طبقة النقل (TLS)، وبروتوكول نقل الملفات الآمن (SFTP)، وبروتوكول النقل الآمن (SSHv2)، وغيرها.

٦-٧ أمن البيئة الافتراضية (Virtual Security)

الهدف

تحديد المتطلبات الهامة للخوادم الموجودة في البيئة الافتراضية لضمان تصميم الخوادم الافتراضية وإعدادها وتشغيلها بطريقة آمنة.

المخاطر المحتملة

يعتبر الإعداد الخاطئ والتصميم الضعيف للبيئة الافتراضية والافتقار إلى الأنظمة الافتراضية الآمنة من الثغرات الأمنية التي يمكن استغلالها لتهديد سرية وسلامة وتوافر بيانات جامعة الملك فيصل وسير عملها.

الإجراءات المطلوبة

١- إعداد وضبط الحدود لكافة أشكال استخدام مصادر البيئة الافتراضية الموجودة على الخوادم.

٢- تطبيق حل إعدادات الخوادم الافتراضية مركزي.

٣- فصل الأجهزة الطرفية غير المستخدمة في بيئة الأنظمة الافتراضية لكافة الخوادم.

٤- تطبيق وإعداد جدار الحماية وخصائص منع التسلل والاختراق للحركة بين الخوادم الافتراضية حتى لو كانت موجودة في نفس الخادم أو المستضيف المادي (الحركة بين الخوادم "East-West traffic").

٥- إعداد شبكات محلية افتراضية (VLANs) للاتصال بين الخادم المستضيف والخادم الضيف بصورة تختلف عن الاتصالات بين الخوادم الافتراضية.

٦- إعداد متحكم منفصل بواجهة شبكة (NIC) في جميع الخوادم الافتراضية للإدارة المتصلة بشبكة افتراضية محلية مستقلة للإدارة.

٧- إعداد بروتوكولات الإنترنت الثابتة على الخوادم الافتراضية.

٨- استخدام البروتوكولات الإدارية التي تدعم التشفير مثل أمن طبقة النقل (TLS)، وبروتوكول النقل الآمن (SSH)، وبروتوكول نقل النص التشعبي الآمن (HTTPS)، وغيرها.

٩- تقييد إدارة بيئة الأنظمة الافتراضية وحصرها على المشرفين المعنيين فقط. تشمل إدارة الأنظمة الافتراضية:

- إنشاء الخوادم الافتراضية وتثبيتها وبدء تشغيلها ونقلها وإغلاقها وإزالتها.
- إعداد وتغيير المتحكم بواجهة الشبكة (NIC) والشبكة المحلية الافتراضية (VLAN) ومفتاح التحويل الافتراضي (Vswitch).
- إدارة الخوادم الافتراضية وإعدادات الوصول.

١٠- عمل نسخة احتياطية على الخوادم الافتراضية وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة الملك فيصل.

١١- إلغاء تفعيل مشاركة الملفات بين البيئات الافتراضية للخوادم والمستضيف.

١٢- تطبيق وإعداد نظام أمان ذو طبقة مزدوجة للبيئة الافتراضية وعزل بيئة الإنتاج عن بيئات الاختبار الافتراضية.

١٣- إعداد شعارات التحذير والتصريح على خوادم المضيف والضيف لإنذار الأشخاص غير المصرح لهم من الاستخدام غير السليم للخادم.

١٤- تسجيل جميع الأنشطة المتعلقة بالأجهزة الافتراضية بما في ذلك الإنشاء، والنشر، والترحيل، والحذف.

٨-٦ إدارة الخوادم (Central Management)

الهدف

تحديد المتطلبات الأمنية لإدارة الخوادم لضمان إدارة وتشغيل الخوادم بطريقة آمنة وضمان تطبيق وتنفيذ جميع المتطلبات الأمنية.

المخاطر المحتملة

يؤدي الافتقار إلى الإدارة الآمنة وعدم تطبيق المتطلبات الأمنية على الخوادم إلى زيادة احتمالية التعرض للهجمات ووجود الثغرات ونقاط الضعف في بيئة جامعة الملك فيصل، حيث يمكن استغلال هذه الثغرات في الهجمات أو الاختراقات الخبيثة التي تعرض الخوادم والبيانات في جامعة الملك فيصل إلى انتهاكات أمنية.

الإجراءات المطلوبة

١- إعداد خادم الإدارة المركزية أو خادم النطاق ليطبق سياسات الإعدادات والتحصين المعتمدة في جامعة الملك فيصل على جميع الخوادم.

٢- تثبيت أدوات إدارة إعدادات النظام التي تقوم تلقائياً بتنفيذ وإعادة تثبيت إعدادات الضبط والتهيئة للأنظمة في فترات زمنية محددة ومنتظمة.

٣- تطبيق نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة محتوى الأمن"SCAP" (Security) Content Automation Protocol للتأكد من عناصر الإعدادات الأمنية كافة وجدولة الاستثناءات المعتمدة والإبلاغ عن حدوث أي تغييرات غير مصرّح بها.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.

قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٧. معيار أمن قواعد البيانات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بأنظمة إدارة قواعد البيانات (Database Management System "DBMS") الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية، وهي: سرية المعلومات، وسلامتها، وتوافرها.

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أنظمة إدارة قواعد البيانات (DBMS) الخاصة بجامعة الملك فيصل، وينطبق على جميع العاملين في جامعة الملك فيصل.

المعايير

I-٧ مراجعة الإعدادات والتحصين (Secure Hardening Configuration)

الهدف

تحديد متطلبات حماية نظام إدارة قواعد البيانات (DBMS) الأساسية لضمان تصميم نظام إدارة قواعد البيانات (DBMS) وإعداده وتشغيله بطريقة آمنة.

المخاطر المحتملة

تعتبر الأخطاء في إعداد نظام إدارة قواعد البيانات (DBMS) والتصاميم الضعيفة من أبرز الأسباب التي تؤدي إلى وجود ثغرات أمنية يمكن استغلالها لتهديد سرية بيانات جامعة الملك فيصل وسلامتها وتوافرها.

الإجراءات المطلوبة

١- مراجعة الجوانب الأمنية لتصميم تقنيات نظام إدارة قواعد البيانات (DBMS) الجديدة واعتمادها من قبل الطرف المعني المصرّح له قبل التثبيت.

٢- توثيق كافة الخدمات والتطبيقات والأدوات التي يمكنها الوصول إلى قواعد البيانات وحفظها، على أن تشمل الوثائق وصفاً موجزاً لاحتياجات العمل.

٣- وضع المكونات المادية للخوادم التي تستضيف نظام إدارة قواعد البيانات (DBMS) في بيئة آمنة ومغلقة ومراقبة.

٤- وضع خوادم نظام إدارة قواعد البيانات (DBMS) وراء جدار حماية لمراقبة الحركة من وإلى خادم قاعدة البيانات.

٥- يجب أن تسمح قواعد جدار الحماية بالوصول الى تطبيقات أو خوادم ويب محدّدة فقط وتمنع ما دون ذلك. كما يجب منع الوصول المباشر إلى خوادم أنظمة إدارة قواعد البيانات (DBMS) الموجودة على الشبكات الداخلية الخاصة بجامعة الملك فيصل، ومنع كافة أنواع الاتصال الأخرى.

٦- تقييد الوصول عن طريق الشبكة إلى خوادم نظام إدارة قواعد البيانات (DBMS) وحصره على مصادر شبكة محدودة مثل خوادم الويب وخوادم التطبيقات وشبكات منطقة التخزين.

٧- العزل المادي أو المنطقي لقواعد البيانات في بيئة الإنتاج عن قواعد البيانات في البيئات الأخرى مثل بيئة الاختبار وبيئة التطوير.

٨- عدم استخدام البيانات الموجودة في قواعد بيانات الإنتاج عند اختبار أو تطوير بيئات قواعد البيانات، مع التأكيد على تطبيق ضوابط أمن سيبراني مثل التعتيم (mask) أو مزج (scramble) البيانات الحسّاسة قبل استخدامها في بيئتي الاختبار أو التطوير.

٩- تمييز طريقة التسمية بين خوادم نظام إدارة قواعد البيانات (DBMS) الإنتاجية وغير الإنتاجية.

١٠- تخصيص خوادم نظام إدارة قواعد البيانات (DBMS) وعدم استضافة أي وظائف أخرى مثل "مستوى الويب أو التطبيق" (Web or Application Tier) أو "خدمات النطاق" (Domain Services).

١١- يجب إعادة تسمية جداول قواعد البيانات الافتراضية.

١٢- تحصين كافة أنظمة التشغيل التي تستضيف قاعدة (أو قواعد) البيانات، وذلك وفقاً لمعيار أمن الخوادم.

١٣- استخدام الإجراءات المخزّنة المتوفّرة للتطبيق فقط لإجراء التعاملات أو الاستفسارات من قواعد البيانات.

١٤- عدم تحديد روابط خوادم نظام إدارة قواعد البيانات (DBMS) (مثل إنشاء اتصالات أو واجهات) بين أنظمة إدارة قواعد البيانات (DBMS) الإنتاجية وغير الإنتاجية.

١٥- استخدام خاصية التحقّق من البيانات لضمان سلامة البيانات المخزّنة.

١٦- تقييد حقول قاعدة البيانات بمجالات محدّدة من المدخلات واستخدام المدخلات الثنائية أو طرق التحقّق الأخرى من المدخلات، مثل التحقّق من الحدود Checking (Boundary)، أو التحقق من المحتوى وتصفية روابط مواقع الإنترنت (Content Inspection/URL Filtering)، لمنع أو الحد من العمليات التالية:

- البيانات المفقودة أو غير المكتملة أو كلاهما
- القيم خارج النطاق
- البيانات غير المصرّح بها أو غير المتسقة
- الأحرف والأرقام غير الصحيحة في حقول البيانات
- تجاوز حدود قيمة الحد الأعلى أو الأدنى للتاريخ

١٧- تقييد الوصول إلى ملفات إعدادات نظام إدارة قواعد البيانات (DBMS) والشفرة المصدرية (Source Code) للتطبيقات والبرمجيات المخزّنة في قاعدة البيانات ومراقبتها.

١٨- استخدام البرمجيات المرخّصة فقط والتي تم التحقّق من صحتها من المورّد في خوادم قواعد البيانات.

١٩- استخدام إصدارات نظام إدارة قواعد البيانات (DBMS) التي يدعمها المورّد فقط.

٢٠- تطبيق كافة التحديثات والإصلاحات الأمنية المناسبة قبل تثبيت نظام إدارة قواعد البيانات (DBMS) في الخدمة، وذلك وفقاً لسياسة إدارة التحديثات والإصلاحات.

٢١- إلغاء تفعيل البرمجة النصية (Scripting) من طرف الخادم على كافة قواعد البيانات إن لم تكن ضرورية.

٢٢- إلغاء تفعيل أو تقييد الوصول إلى البرامج والملفات التنفيذية الخارجية.

٢٣- حذف الرموز والملفات والأوامر الافتراضية وغيرها التي لم تعد ضرورية بعد تثبيت نظام إدارة قواعد البيانات (DBMS).

٢٤- إلغاء تفعيل كافة الخدمات أو المنافذ غير الضرورية أو حذفها من خوادم قواعد البيانات.

٢٥- ضبط إعدادات قواعد البيانات لاستقبال اتصالات الشبكة على الواجهات (Interfaces) المصرّح بها فقط.

٢٦- يجب التأكد من سلامة حزم تحديثات وإصلاحات برمجيات قواعد البيانات وفقاً لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة في جامعة الملك فيصل.

٢٧- حفظ قائمة جرد دقيقة لكافة قواعد البيانات ومحتوياتها وتحديثها دورياً.

٢٨- ترميز البيانات المخزّنة في قواعد البيانات باستخدام أنواع ترميز آمنة محدّدة مسبقاً وفقاً للسياسات والإجراءات ذات العلاقة في جامعة الملك فيصل.

٢-٧ تأمين الوصول (Secure Access)

الهدف

تطبيق ضوابط التحقّق والتصريح ذات العلاقة والمحدّدة لضمان منح حق الوصول إلى نظام إدارة قواعد البيانات (DBMS) وصلاحيات استخدامه بناءً على الحاجة إلى المعرفة والحاجة إلى التنفيذ.

المخاطر المحتملة

يمكن أن يؤدي الوصول غير المصرّح به إلى نظام إدارة قواعد البيانات (DBMS) أو صلاحيات استخدامه غير الضرورية إلى إفصاح غير مصرّح به أو تغييرات غير معتمدة على بيانات جامعة الملك فيصل وتعطيل سير العمل.

الإجراءات المطلوبة

١- استخدام آليات آمنة فقط للتحقّق من هويات المستخدمين للوصول إلى قواعد البيانات مثل التحقق من الهوية متعدد العناصر والذي يتضمن مجموعة من عناصر التحقق مثل:

- المعرفة (ما يعرفه المستخدم فقط "مثل كلمة المرور")
- الحيازة (ما يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول")
- الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع")

٢- استخدام أنظمة التحكّم في الوصول لإدارة الوصول إلى نظام إدارة قواعد البيانات (DBMS).

٣- التحقّق من هوية المستخدم أو التطبيق الذي يطلب الوصول إلى نظام إدارة قواعد البيانات (DBMS) قبل منحه حق الوصول.

٤- تغيير كلمات المرور الافتراضية للحسابات والخدمات (مثل "SA" و"Listener") قبل تثبيتها.

٥- عدم السماح للحسابات الافتراضية (مثل "SA" و"PUBLIC") بالبقاء نشطة، حيث يجب أن تخضع هذه الحسابات إلى الإجراءات التالية:

- تغيير اسمها أو حذفها أو إلغاء تفعيلها (حسب الحاجة).
- عدم منح الحسابات الافتراضية التي يمكن حذفها (أو إلغاء تفعيلها) امتيازات وصلاحيات لاستخدام نظام إدارة قواعد البيانات (DBMS) إلا إذا اشترط المورّد ذلك مباشرةً.
- في حال عدم التمكّن من تغيير اسم الحساب الافتراضي أو حذفه أو إلغاء تفعيله، يجب تقييد الوصول له وفقاً لسياسة إدارة الوصول.
- منع الوصول المباشر إلى هذه الحسابات/الوظائف (التي لا يمكن تغيير اسمها أو حذفها أو إلغاء تفعيلها) والطلب من المستخدم تسجيل الدخول من خلال حسابه الخاص ذي الامتيازات والصلاحيات الإدارية.

٦- تطبيق سياسات التحكّم في الوصول التقديرية (Control Discretionary Access)، على النحو الذي حدّده مالك البيانات، على المستخدمين والأوامر المحدّدة (Subjects and Objects).

٧- الحفاظ على الفصل بين المهام في جميع أنظمة إدارة قواعد البيانات (DBMS)، وعدم استخدام مشرفي قواعد البيانات (DBA) حسابات المديرين/حسابات المستخدمين عالية الامتيازات (Admins/Super User Accounts) في الأنشطة اليومية.

٨- تقييد الوصول إلى الحسابات ذات الإمكانات الإدارية وحصره على عددٍ قليل من الأفراد المصرّح لهم حسبما هو مطلوب لإدارة نظام إدارة قواعد البيانات (DBMS) والتطبيقات.

٩- تطبيق مبدأ الحد الأدنى من الصلاحيات على الوصول إلى نظام إدارة قواعد البيانات (DBMS) وتقييد التصاريح اللازمة لأداء الوظائف في قاعدة البيانات بناءً على الأدوار والمسؤوليات الوظيفية، وإدارة التصاريح من خلال الأدوار أو المجموعات وليس من خلال التصاريح المباشرة الممنوحة إلى هويات المستخدم.

١٠- تقييد قدرة مستخدمي قواعد البيانات على الوصول إلى محتويات قواعد البيانات أو إدراجها أو تعديلها أو حذفها بناءً على مهامهم في العمل.

١١- تجنب تشغيل خدمات نظام إدارة قواعد البيانات (DBMS) على نظام التشغيل الخاص بالمستضيف من خلال حسابات ذات امتيازات وصلاحيات.

١٢- يجب على مديري قواعد البيانات (DBA) استخدام حسابات فردية لأداء المهام الإدارية وعدم استخدام حساب مشترك أو جماعي.

١٣- تطبيق أدوار الوصول على الجداول الافتراضية (Views) وقواعد البيانات، لتجنّب المخاوف المتعلّقة بمجموع أو تجميع بيانات منفصلة ضمن قواعد البيانات والتي يمكن أن تتيح للمستخدم تحديد المعلومات الحسّاسة أو المصنّفة.

١٤- عدم إعداد قواعد البيانات بكلمات مرور فارغة.

١٥- استخدام كلمات مرور قوية لكافة أنظمة التشغيل وحسابات قاعدة البيانات الخاصة بمدير قاعدة البيانات وتغييرها عند ترك المشرفين أو المتعاقدين مناصبهم حسب ما تنص عليه سياسة إدارة هويات الدخول والصلاحيات.

١٦- حذف الملفات المؤقّتة (من عملية التثبيت) والتي يمكن أن تحتوي على كلمات مرور.

١٧- تقييد الوصول إلى ملفات قواعد البيانات وحصره على العمليات ذات العلاقة والمستخدمين الإداريين المصرّح لهم.

١٨- إغلاق جلسة المستخدم تلقائياً بعد تلبية الشروط المحدّدة مثل انتهاء مهلة الجلسة.

٣-٧ سجلات التدقيق (Audit Logs)

الهدف

إصدار سجلات نظام إدارة قواعد البيانات (DBMS) للأحداث الأمنية الرئيسية والحرجة وتسجيلها وتأمينها على نظام إدارة قواعد البيانات (DBMS) للمساعدة في التحقيق والتتبع والتحقّق في المستقبل.

المخاطر المحتملة

تَحُد سجلات التدقيق غير الوافية من قدرة جامعة الملك فيصل على كشف الانتهاكات والحوادث والمسائل الأمنية وتتبُّعِها في نظام إدارة قواعد البيانات (DBMS)، وتُقيّد إمكانية تحديد سبب الانتهاكات الأمنية. كما يؤدي عدم تأمين سجلات التدقيق على نظام إدارة قواعد البيانات (DBMS) بالشكل المناسب إلى العبث بالسجلات مما يؤثّر في سلامتها.

الإجراءات المطلوبة

١- مزامنة أوقات جميع أنظمة إدارة قواعد البيانات (DBMS) مع خادم بروتوكول وقت الشبكة (Network Time Protocol) المركزي.

٢- يمكن إرفاق السجلات بسجلات نظام التشغيل أو أن تكون مستقلّة ضمن نظام إدارة قواعد البيانات (DBMS).

٣- إصدار سجلات التدقيق التي تحتوي على معلومات كافية لتحديد هوية أي مستخدم أو عملية ذات علاقة بالحدث المعني.

٤- تسجيل نشاطات نظام إدارة قواعد البيانات (DBMS) التالية بحدّ أدنى:

- جميع حالات الإنذار أو الأخطاء التي ظهرت في النظام.
- التشغيل.
- الإغلاق.
- إنشاء أو تعديل أو حذف (استبعاد) قواعد البيانات وأي هيكل تخزين لقواعد البيانات وأي جداول لقواعد البيانات وفهارس وحسابات ومصادر.
- تفعيل وظيفة التدقيق وإلغاء تفعيلها.
- منح الامتيازات والصلاحيات وإلغائها على مستوى نظام إدارة قواعد البيانات (DBMS).
- أي إجراء يُسبِّب ظهور رسالة خطأ لعدم وجود المصدر الذي يتم البحث عنه.
- أي إجراء يؤدي إلى إعادة تسمية مصدر على نظام إدارة قواعد البيانات (DBMS).
- أي إجراء يمنح أو يلغي امتيازات وصلاحيات استخدام المصدر من دور أو حساب نظام إدارة قواعد البيانات (DBMS).
- الأختام الزمنية عند وقوع الأحداث.
- كافة التعديلات على دليل البيانات أو إعدادات نظام إدارة قواعد البيانات (DBMS).
- تدقيق جميع حالات فشل الاتصال بنظام إدارة قواعد البيانات (DBMS) حيثما أمكن، ويضمن مدير قاعدة البيانات تدقيق محاولات الاتصال الناجحة وغير الناجحة.
- محاولات تسجيل الدخول غير الناجحة، وأقفال كلمات المرور.
- محاولات إضافة، أو تعديل، أو حذف الامتيازات، والصلاحيات، أو التصاريح.
- حذف فئات من المعلومات (مثل مستويات التصنيف أو مستويات الأمن).
- أمر غير عادي (أمر يطلب أمراً آخر وهكذا).
- إلغاء تفعيل سجلات نظام إدارة قواعد البيانات (DBMS) أو تعديلها.

٥- توفير تنبيه فوري ومباشر من أجل تقديم الدعم المناسب للأشخاص في جميع أحداث فشل التدقيق التي تتطلّب إجراءات مباشرة.

٦- حماية خصائص التدقيق في نظام إدارة قواعد البيانات (DBMS) من عمليات الحذف غير المصرّح بها.

٤-٧ التعافي من الكوارث والنسخ الاحتياطية (Disaster Recovery and Backup)

الهدف

تحديد متطلّبات عمل نسخ احتياطية لقواعد البيانات واختبارها (مثل النموذج والوتيرة والنوع) لضمان توافر البيانات المخزّنة في قاعدة البيانات بمستوى مقبول لدى جامعة الملك فيصل في حال حدوث عطل كبير.

المخاطر المحتملة

في حال حدوث عطل كبير في البنية التحتية الخاصة بجامعة الملك فيصل، بما في ذلك نظام إدارة قواعد البيانات (DBMS)، ولم تتوفر نسخ احتياطية سليمة، فإن جامعة الملك فيصل لن تكون قادرة على استئناف عملها بالصورة المطلوبة.

الإجراءات المطلوبة

١- عمل نسخ احتياطية لقاعدة البيانات دورياً بناءً على احتياجات العمل ووفقاً لمتطلّبات خطة استمرارية الأعمال (BCP) وخطة التعافي من الكوارث (DRP).

٢- اختبار البيانات المخزّنة والتي تم عمل نسخ احتياطية لها والتحقّق منها وتحديثها كل ثلاثة أشهر أو وفقاً لإجراءات اختبار خطة التعافي من الكوارث (DRP).

٣- عمل نسخ من نظام إدارة قواعد البيانات (DBMS) (نسخ احتياطية تابعة) لجميع أنظمة قواعد البيانات المتواجدة خارج الموقع أو المستضافة على الخدمات السحابية (داخل المملكة العربية السعودية).

٤- الاحتفاظ بالنسخ الاحتياطية من قاعدة البيانات لفترات زمنية معتمدة تكون كافية لتلبية متطلّبات استئناف العمل (كما ورد في ضوابط الأنظمة الحساسة "ECC-2-9-2" و"CSCC-2-8-1" و"CSCC-2-8-2") وذلك لمدّة ١٢ شهراً لجميع قواعد البيانات و١٨ شهراً لقواعد بيانات الأنظمة الحساسة.

٥-٧ التشفير (Cryptography)

الهدف

تحديد متطلّبات تشفير نظام إدارة قواعد البيانات (DBMS) (بما في ذلك الاتصالات والتحقّق والتخزين) وتحديد متطلّبات البروتوكولات الآمنة وشهادات التشفير المعتمدة.

المخاطر المحتملة

قد يعرّض عدم استخدام نظام إدارة قواعد البيانات (DBMS) لآليات تشفير مُحكَمة جامعة الملك فيصل لإفصاح غير مصرّح به عن البيانات الحسّاسة.

الإجراءات المطلوبة

١- تشفير قواعد البيانات وفقاً لسياسة التشفير لمنع التعديل غير المصرّح به على البيانات المصنّفة والخاصة المخزّنة.

٢- تشفير قواعد البيانات وفقاً للمعايير والسياسات ذات العلاقة (يرجى الرجوع إلى سياسة تصنيف البيانات ومعيار التشفير المعتمد).

٣- نقل البيانات عبر الشبكة وبين الأنظمة باستخدام آليات تشفير قوية وكافية للحدّ من مخاطر انتهاك البيانات.

٤- تشفير ملفات قاعدة البيانات، على مستوى قاعدة البيانات أو على مستوى الحقول، وفقاً للسياسات والإجراءات ذات العلاقة في جامعة الملك فيصل.

٥- حماية مفاتيح التشفير وفقاً لسياسة التشفير.

٦- التحقّق من شهادات التشفير من المزوّد وهيئة منح الشهادات (CA) المعنية.

٧- تشفير أشرطة النسخ الاحتياطية التي تُخزّن النسخ الاحتياطية من قواعد البيانات وعدم تخزين مفتاح التشفير على نفس الأشرطة في حالة غير مشفرة.

٨- تشفير كافة حركات (Traffic) المديرين أو المستخدمين أو التطبيقات من نظام إدارة قواعد البيانات (DBMS) وإليه.

٩- عدم استخدام بروتوكولات غير مشفّرة أو خدمات غير آمنة (مثل بروتوكول نقل النص التشعبي "HTTP"، وبروتوكول نقل الملفات "FTP"، وغيرها) واستخدام بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وغيرها بدلاً منها.

١٠- حساب القيمة المميزة (Hash) لعبارات المرور المخزّنة في قواعد البيانات باستخدام خوارزمية مُحكَمة وعشوائية بصورة فريدة (Uniquely Salted) لحساب النص المميز (Hash Function) بصورة فريدة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٨. معيار إدارة الثغرات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من خلال الهجمات السيبرانية، والتقليل من الآثار الناتجة عن هذه الهجمات على أعمال جامعة الملك فيصل، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-١٠-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية في جامعة الملك فيصل، وينطبق على جميع العاملين في جامعة الملك فيصل.

المعايير

٨-١ المتطلبات العامة

الهدف

تحديد المتطلبات العامة لتقييم الثغرات التي يجب أن يتبعها فريق تقييم الثغرات الداخلي أو الخارجي قبل بدء عملية تقييم الثغرات.

المخاطر المحتملة

يمكن أن يؤدي تقييم الثغرات غير المخطط له بشكل صحيح إلى مخرجات غير كافية أو غير دقيقة، أو قد تؤثر عملية تقييم الثغرات على كفاءة الأنظمة والخدمات.

الإجراءات المطلوبة

١- يجب إعداد خطة لتقييم الثغرات يوضح فيها نطاق العمل وتاريخ البدء والانتهاء.

٢- يجب التأكد من أن خطة تقييم الثغرات متوافقة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٣- ينبغي التأكد من أن نشاط إدارة الثغرات (والذي يشمل الاكتشاف والفحص والتصنيف والمعالجة) يسير وفقاً لمنهجية محددة ووفقاً لنماذج سياسات وإجراءات وعمليات إدارة مخاطر الأمن السيبراني والمخاطر المؤسسية المعتمدة في جامعة الملك فيصل.

٤- ينبغي صياغة تقرير بعد الانتهاء من نشاط تقييم الثغرات. ويجب أن يتضمن التقرير الأقسام التالية على الأقل:

- الملخص التنفيذي.

- مقدمة لإعداد التقارير.
- المنهجية.
- الأصول المستهدفة.
- تقرير تفصيلي لنتائج تقييم الثغرات.

٥- بعد الانتهاء من تقرير تقييم الثغرات، يجب إعداد خطة عمل لتنفيذ التوصيات، على أن يتضمن التقرير ما يلي على الأقل:

- المسؤول التقني عن الأصل (Technical Owner).
- مالك الأصل (Business Owner).
- الإجراءات المطلوبة لتنفيذ التوصيات.
- الفترة الزمنية اللازمة لتنفيذ التوصيات.

٦- ينبغي مقارنة نتائج تقييم الثغرات مع النتائج السابقة للتأكد من معالجة الثغرات السابقة في الوقت المحدد.

٢-٨ آلية تقييم الثغرات

الهدف

تحديد ووضع خطة لوسائل تقييم الثغرات والأدوات المستخدمة التي يجب أن يتبعها فريق تقييم الثغرات الداخلي أو الخارجي قبل بدء عملية تقييم الثغرات.

المخاطر المحتملة

قد يؤدي تقييم الثغرات من غير آلية واضحة ومعتمدة إلى نتائج غير واضحة أو غير دقيقة، وبالتالي قد تُستغل تلك الثغرات قبل اكتشافها وأيضاً قد تتسبب بإهدار الموارد والوقت.

الإجراءات المطلوبة

١- يجب إجراء تقييم الثغرات دورياً أو مرة واحدة في السنة على الأقل.

٢- يجب إجراء تقييم الثغرات مرة واحدة شهرياً للمكونات التقنية للأنظمة الحساسة الخارجية. (CSCC-2-9-1-2)

٣- يجب إجراء تقييم الثغرات مرة واحدة كل ثلاثة أشهر للمكونات التقنية للأنظمة الحساسة الداخلية. (CSCC-2-9-1-2)

٤- يجب التأكد من تنفيذ تقييم الثغرات وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، مع الأخذ بالاعتبار الإرشادات التالية:

- توفير المتطلبات الخاصة ببدء فحص واكتشاف الثغرات الواردة في إجراءات إدارة الثغرات.
- تحديد المكونات التقنية المستهدفة بالفحص وتوفير الصلاحيات اللازمة للقيام بفحص واكتشاف الثغرات.
- التأكد من أن عملية فحص واكتشاف الثغرات تغطي ثغرات الشبكة وثغرات الخدمات والرسائل النصية التعريفية (Banner Grabbing).

- إجراء فحص واكتشاف ثغرات عن طريق وسائل وتقنيات معتمدة.
- تصنيف الثغرات حسب خطورتها ووفقاً لمنهجية إدارة المخاطر السيبرانية.

٣-٨ معالجة الثغرات

الهدف

تحديد آلية لمعالجة الثغرات بشكل فعّال ومنع أو تقليل احتمالية استغلال هذه الثغرات، وتقليل الآثار الناتجة عن هذه الهجمات على سير الأعمال.

المخاطر المحتملة

قد يؤدي عدم معالجة الثغرات إلى استغلال تلك الثغرات واستخدامها لشن هجمات سيبرانية.

الإجراءات المطلوبة

١- يجب إعداد خطة لمعالجة الثغرات على المكونات التقنية المستهدفة توضح فيها تفاصيل الثغرات والتوصيات وتاريخ البدء وتاريخ الانتهاء والإدارات/المشرفين المعنيين بمعالجة الثغرات.

٢- يجب توثيق خطة العمل واعتمادها من قبل إدارة الأمن السيبراني.

٣- يجب أن تكون جميع المكونات التقنية لدى جامعة الملك فيصل مضمونة ومدعومة من قبل المورد/المصنّع وفقاً لاتفاقية مستوى الخدمة مع المورد/المصنّع.

٤- يجب أن تكون لجميع المكونات التقنية الموجودة لدى جامعة الملك فيصل حزم تحديثات وإصلاحات أمنية محدثة على مستوى نظام التشغيل والتطبيقات.

٥- من المستحسن أن يتم توفير تقنيات أتمتة (إن وجدت) تحديثات أنظمة التشغيل والبرامج (بما في ذلك برامج الأطراف الخارجية) داخل جامعة الملك فيصل.

٦- يجب معالجة الثغرات الحرجة (Critical Vulnerabilities) فور اكتشافها ووفقاً لآليات إدارة التغيير المعتمدة لدى جامعة الملك فيصل. ينبغي أن تكون لجميع الثغرات التي تشكل مخاطر مرتفعة أو متوسطة خطة عمل لإغلاقها ومعالجتها خلال أسبوعين كحد أقصى من تاريخ إصدار الإصلاح أو حزمة التحديثات والإصلاحات من قبل المورد، إلا إذا كان هناك مبرر تقني أو مبرر بناءً على احتياجات العمل يمنع ذلك وتم التبليغ عنه رسمياً.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني** .
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني**.
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني** وإدارة الأمن السيبراني.

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

٩. معيار إدارة حوادث وتهديدات الأمن السيبراني

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حوادث وتهديدات الأمن السيبراني الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-١٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار كافة الأصول المعلوماتية والتقنية الخاصة بجامعة الملك فيصل، وينطبق على جميع العاملين في جامعة الملك فيصل.

المعايير

٩-١ خطط الاستجابة للحوادث (Incident Response Plans)

الهدف

ضمان التطبيق الملائم لمنهجية بشكل رسمي ومركز ومتناسق وتشكيل خارطة الطريق لتنفيذ عمليات الاستجابة للحوادث في جامعة الملك فيصل في حال التعرض لهجوم يستهدف البيانات الشخصية وبيانات العمل.

المخاطر المحتملة

في حال عدم وضع خطة استجابة للحوادث وتطبيقها في جامعة الملك فيصل، قد تواجه الجامعة المخاطر المحتملة التالية:

- الإخفاق في الاستجابة بشكل مُمنهج (أي باتباع منهجية شاملة في التعامل مع الحوادث) للحوادث التي قد تؤدي إلى إتلاف المعلومات أو سرقتها أو الوصول غير المصرح به إليها أو الإفصاح عنها مما يمكن أن يؤدي إلى انقطاع الخدمات.
- عدم القدرة على التعامل بكفاءة مع الحوادث التي يمكن أن تؤدي إلى مخاطر قد تؤثر على سمعة جامعة الملك فيصل.
- عدم الاستفادة من المعلومات أثناء التعامل مع الحوادث من أجل التحضير بشكل أفضل للتعامل مع الحوادث المستقبلية وتوفير حماية أعلى للأنظمة والبيانات.
- اتباع منهجية ضعيفة في التعامل مع القضايا القانونية التي قد تنشأ خلال الحوادث وتهديدات الأمن السيبراني.

الإجراءات المطلوبة

١- تطوير خطة تلبي متطلبات الأعمال الخاصة بجامعة الملك فيصل، وترتبط بالمهام والحجم والهيكلية والوظائف الخاصة بجامعة الملك فيصل، وتحدد الموارد اللازمة والدعم الإداري المطلوب.

٢- تحديد عاملين إداريين، إضافة إلى من ينوبهم عند الحاجة، لتوفير الدعم اللازم في عمليات التعامل مع الحوادث من خلال تولي الأدوار الرئيسية لاتخاذ القرارات.

٣- دراسة العوامل ذات العلاقة عند اختيار هيكلية فريق الاستجابة للحوادث في سياق احتياجات جامعة الملك فيصل والموارد المتوفرة. ومن أمثلة هيكلية فريق الاستجابة للحوادث التالي:

- الفريق المركزي للاستجابة للحوادث والذي يتألف من فريق واحد يتعامل مع الحوادث في كافة جهات وقطاعات جامعة الملك فيصل.
- الفرق الموزعة للاستجابة للحوادث والتي تتألف من العديد من فرق الاستجابة للحوادث، حيث يكون كل فريق منها مسؤولاً عن شريحة منطقية أو مادية معينة في جامعة الملك فيصل.

٤- تحديد هيكلية فريق الاستجابة للحوادث الذي يجب أن يكون متوفراً لمساعدة أي فرد يكتشف أو يشتبه بوقوع حادثة لها علاقة بجامعة الملك فيصل.

٥- اختيار الأفراد الذين يملكون المهارات الفنية والخبرة والكفاءة المطلوبة للعمل في فريق الاستجابة للحوادث وتمكينه من القيام بأنشطة الاستجابة للحوادث إلى جانب الأنشطة التالية:

- كشف الاختراقات: يتوقع من الفريق تحليل الحوادث بسرعة ودقة بناءً على المعرفة المكتسبة من تقنيات كشف الاختراقات.
- تقديم الاستشارات: يمكن أن يقدم الفريق الاستشارات لجامعة الملك فيصل فيما يتعلق بالثغرات والتهديدات الجديدة. وعادةً ما تكون الاستشارات مطلوبة عند ظهور تهديدات جديدة مثل الأحداث السياسية البارزة.
- رفع مستوى الوعي والتوعية: أن يكون المستخدمون والعاملون الفنيون على اطلاع بكيفية كشف الحوادث والإبلاغ عنها والاستجابة لها. ويمكن تحقيق هذا من خلال وسائل مختلفة مثل ورشات العمل والمواقع الإلكترونية والنشرات الإخبارية والملصقات.
- مشاركة المعلومات: يشارك فريق الاستجابة للحوادث عادة في مجموعات مشاركة المعلومات.

٦- إدراج التفاصيل في التحليل الأولي عند وقوع حادثة أمنية وذلك لتحديد نطاقها. وتشمل هذه التفاصيل الشبكات أو الأنظمة أو التطبيقات المتأثرة، والمتسبب بالحادثة، وكيفية وقوعها (مثل الأدوات أو طرق الهجوم المستخدمة والثغرات المستغلة). كما يجب أخذ ما يلي بعين الاعتبار عند إجراء التحليل الأولي:

- تحديد خصائص الشبكات والأنظمة التي تم قياس خصائص النشاط المتوقع فيها بحيث يكون من السهل تحديد التغييرات.
- فهم السلوكيات الطبيعية.
- استخدام سجل مركزي وصياغة سياسة الاحتفاظ بالسجلات.
- ربط الأحداث مع بعضها البعض.
- الحفاظ على تزامن ساعات المستضيف.

- الحفاظ على قاعدة معرفية بالمعلومات واستخدامها.
- تشغيل برامج التلصص على المعلومات لجمع معلومات إضافية.
- وضع مصفوفة تشخيص للعاملين الأقل خبرة.

٧- تحديد أولويات الأنشطة اللاحقة، مثل احتواء الحادثة والتحليل العميق لتأثيرات الحادثة، وذلك بناءً على نتائج التحليل الأولي.

٨- توثيق وتسجيل كافة الحقائق المتعلقة بالحادثة عن طريق السجل، أو أجهزة الحاسب المحمولة، أو التسجيلات الصوتية، أو الكاميرات الرقمية.

٩- توثيق وتسجيل توقيت كل خطوة تم اتخاذها من وقت اكتشاف الحادثة وحتى وقت معالجتها، وتأريخ كل وثيقة تتعلق بالحادثة والتوقيع عليها من قبل الجهة المعنية بالتعامل مع الحوادث.

١٠- الاحتفاظ بسجلات حول حالة الحادثة باستخدام تطبيق أو قاعدة بيانات مثل نظام تتبع المشكلات، على أن تتضمن هذه السجلات ما يلي:

- ملخص الحادثة.
- المؤشرات المتعلقة بالحادثة (أي الدلائل التي تشير إلى وقوع الحادثة أو احتمالية وقوعها في المستقبل).
- الإجراءات المتخذة من قبل جميع جهات التعامل مع الحوادث فيما يخص الحادثة.
- تسلسل العهدة، إن كان مطبقاً.
- تقييمات الأثر المتعلقة بالحادثة.
- معلومات الاتصال بالأطراف الأخرى المعنية (مثل الجهات المسؤولة عن النظام، أو مشرفي النظام، أو الموردين).
- قائمة بالأدلة التي تم جمعها خلال التحقيق في الحادثة.
- آراء وتعليقات الجهات المعنية بالتعامل مع الحوادث.
- الخطوات اللاحقة التي سيتم اتخاذها.

١١- وضع معيار لعملية المراجعة المطلوبة من الإدارة العليا لتحديد إمكانية إفصاح جامعة الملك فيصل عن أي معلومات تتعلق بالحادثة الأمنية (مثل الجهة التي أبلغت عن الحادثة/المسببات والأنظمة المتأثرة) إلى أطراف خارجية (باستثناء الهيئة الوطنية للأمن السيبراني).

١٢- حماية بيانات الحادثة وتقييد الوصول إليها إلى جانب تشفير المراسلات المتعلقة بالحادثة (مثل رسائل البريد الإلكتروني).

٢-٩ تصنيف الحوادث وتحديد أولوياتها (Incidents Classification and Prioritization)

الهدف

ضمان الاستجابة الفعالة والملائمة للحوادث بناءً على تقدير أثرها على الأعمال.

المخاطر المحتملة

في حالات الحوادث، يؤدي عدم تحديد الأولويات بصورة صحيحة إلى تسمية غير واضحة لحوادث أمن الشبكات وتنبيهاته ومشكلاته، مما ينتج عنه تأخير في الاستجابة للحوادث الطارئة، وعدم القدرة على تحديد الحوادث التي يمكن التعامل معها باعتبارها غير طارئة أو التنبيهات التي يمكن تجاهلها (مؤشرات سلبية خاطئة)، إلى جانب سوء تقدير نوع الاستجابة المناسب لحوادث وتنبيهات ومشكلات معينة.

الإجراءات المطلوبة

١- تحديد أولويات الاستجابة لكل حادثة بناءً على تقدير أثرها على الأعمال والجهود المطلوبة للتعافي منها. ويجب أخذ العوامل التالية بعين الاعتبار عند دراسة أثر الحادثة:

- الأثر الوظيفي للحادثة: تؤثر الحوادث التي تستهدف أنظمة تقنية المعلومات عادة على وظائف الأعمال التي تقدمها تلك الأنظمة، مما يؤثر سلباً على مستخدميها. يتضمن الجدول رقم ١٠ أمثلة على فئات الآثار الوظيفية التي يمكن لجامعة الملك فيصل استخدامها لتقييم حوادثها.
- الأثر المعلوماتي للحادثة: يمكن أن تؤثر الحوادث على سرية معلومات جامعة الملك فيصل وسلامتها وتوافرها. يتضمن الجدول رقم ١١ أمثلة على فئات الآثار المعلوماتية المحتملة تصف مقدار الانتهاك الأمني الذي تعرضت له المعلومات خلال الحادثة.
- إمكانية التعافي من الحادثة: يحدد حجم الحادثة ونوع الموارد المتأثرة بالحادثة مقدار الوقت والموارد المطلوبة للتعافي منها. يحتوي الجدول رقم ١٢ على فئات الجهد المطلوب للتعافي من الحوادث، وتعكس هذه الفئات مستوى الموارد المطلوبة للتعافي ونوعها.

٢- تصنيف جميع الحوادث بناءً على مستوى الحدة (الجدول رقم ١٣).

٣- إجراء الأنشطة التالية عند محاولة تحديد المستضيف المسؤول عن هجوم الأمن السيبراني:

- التحقق من عنوان بروتوكول الإنترنت للمستضيف المهاجم.
- البحث عن المستضيف المهاجم عن طريق محركات البحث.
- استخدام قاعدة بيانات الحوادث.
- مراقبة قنوات الاتصالات المحتملة التي يستخدمها المهاجم.

٤- تحديد إجراء التصعيد في الحالات التي لا يستجيب فيها فريق الاستجابة للحوادث للحادثة ضمن الإطار الزمني المحدد.

٣-٩ الإبلاغ عن الحوادث (Incident Reporting)

الهدف

ضمان الالتزام التام بأنظمة الهيئة الوطنية للأمن السيبراني أو بما تصدره، وتعزيز جهود جامعة الملك فيصل من خلال توفير حلقة وصل للتعامل مع الحوادث. وتقوم الهيئة الوطنية للأمن السيبراني، إضافة إلى الجهات الأخرى، بتحليل المعلومات التي تقدمها جامعة الملك فيصل لتحديد توجهات الهجمات ومؤشراتها. ويمكن تمييز هذه التوجهات بشكل أدق عند مراجعة بيانات العديد من الجهات مقارنة بمراجعة بيانات جهة واحدة.

المخاطر المحتملة

يعتبر الإخفاق في إبلاغ الهيئة الوطنية للأمن السيبراني عن الحوادث نوعاً من عدم الالتزام بالمتطلبات الرسمية التي حددتها الهيئة الوطنية للأمن السيبراني، والتي تتمحور رسالتها حول مراقبة التزام الجهات باستمرار بهدف دعم الدور الهام للأمن السيبراني. ونظراً إلى أنه يتوجب على جميع الجهات الوطنية تطبيق كافة الإجراءات اللازمة لضمان الالتزام المستمر بالضوابط الأساسية للأمن السيبراني وفقاً للبند ٣ من المادة ١٠ من تكليف الهيئة الوطنية للأمن السيبراني، ووفقاً للأمر السامي الكريم رقم ٥٧٢٣١ بتاريخ ١٤٣٩/١١/١٠، فإن الإخفاق في الإبلاغ عن الحوادث يمكن أن يؤدي إلى عقوبات بحق جامعة الملك فيصل.

الإجراءات المطلوبة

١- تحديد جهة اتصال رئيسية واحتياطية مع الهيئة الوطنية للأمن السيبراني، والإبلاغ عن كافة الحوادث التي تتوافق مع سياسة إدارة حوادث وتهديدات الأمن السيبراني في جامعة الملك فيصل.

٢- تحديد طرق وقنوات الاتصال المطلوبة لاطلاع جامعة الملك فيصل والجهات المعنية الخارجية، مثل الهيئة الوطنية للأمن السيبراني، على آخر المستجدات.

٣- وضع سياسة تحدد المدة الزمنية التي يجب على مشرفي النظام وأفراد فريق العمل الآخرين إبلاغ فريق الاستجابة للحوادث عن الأحداث الشاذة خلالها، وآليات الإبلاغ (بما في ذلك قنوات الإبلاغ مثل رقم الهاتف و/أو عنوان البريد الإلكتروني)، ونوع المعلومات التي يجب إدراجها عند الإبلاغ عن الحوادث.

٤- وضع خطط تدريبية وسيناريوهات استجابة للحوادث وتطبيقها من أجل اختبار قنوات الاتصال التي تستخدمها فرق الاستجابة للحوادث، وتقييم مهارات اتخاذ القرار لديهم إلى جانب قدراتهم الفنية وذلك بهدف زيادة الوعي والمرونة في الاستجابة للتهديدات.

٥- تحديد أطر زمنية معينة والالتزام بها عند إبلاغ الهيئة الوطنية للأمن السيبراني عن حوادث الأمن السيبراني.

٤-٩ خطة التعافي من الحوادث واستمرارية الأعمال (Incident Recovery and Business Continuity Plan)

الهدف

ضمان تعافي واستعادة عمل الأنظمة بشكل طبيعي، واستعادة وظائف المستضيف المتأثر وبياناته، وإلغاء إجراءات الاحتواء المؤقت (في الحوادث المرتبطة بالبرمجيات الضارة)، وضمان توافق إجراءات وسياسات الاستجابة للحوادث وعمليات استمرارية الأعمال، مما يخدم رسالة جامعة الملك فيصل وأهدافها العامة.

المخاطر المحتملة

يمكن أن يؤدي الإخفاق في تطبيق إجراءات خطة التعافي واستمرارية الأعمال بشكل ملائم إلى تكرار الهجمات والحوادث مستقبلاً، مما قد يؤثر على نسبة رضا المعنيين داخلياً وخارجياً، وكذلك المستفيدين من خدمات الجامعة، وما قد يترتب على ذلك من تبعات نظامية.

الإجراءات المطلوبة

١- إصدار بلاغ باستجابة لحادثة أمنية وإسنادها إلى فريق الاستجابة للحوادث عند الإبلاغ عن حادثة أمنية.

٢- القيام بالأنشطة اللازمة لاستعادة الأنظمة المتأثرة، وتشمل هذه الأنشطة على سبيل المثال لا الحصر ما يلي:

- استعادة الأنظمة من النسخ الاحتياطية السليمة.
- إعادة بناء الأنظمة من الصفر.
- استبدال الملفات التي تعرضت لانتهاكات أمنية بنسخ سليمة.
- تثبيت التحديثات والإصلاحات.
- تغيير كلمات المرور وتشديد أمن محيط الشبكة (مثل مجموعة قواعد جدار الحماية، وقوائم التحكم بالوصول إلى مُوجّه الحدود).

٣- ضمان معالجة حادثة الأمن السيبراني وتصحيحها ضمن الأطر الزمنية المحددة، وفي حال عدم القدرة على ذلك، يجب على فريق الاستجابة للحوادث تصعيد الحادثة وفقاً لتصنيف الحوادث الأمنية وقواعد وإجراءات تصعيد الحوادث المعتمدة في إدارة الأمن السيبراني.

٤- تخصيص الجامعة للميزانية والموارد اللازمة للتعافي من حوادث الأمن السيبراني، وذلك من خلال توفير التمويل اللازم والسريع من أجل التقليل من الأضرار والتعافي من الحوادث السيبرانية.

٥- في بعض الحالات، يجب أن تدرس الجهات المعنية بالتعامل مع الحوادث الجهد المطلوب للتعافي فعلياً من الحادثة، وتقارن هذا الجهد بالقيمة الناتجة عن جهود التعافي، وأي متطلبات مرتبطة بالتعامل مع الحوادث.

٦- تخزين تفاصيل حوادث الأمن السيبراني التي تقع (مثل نوع الحادثة وفئتها، والمستخدمين الذين أبلغوا عنها، والخدمات والأصول والمعلومات المتأثرة بها، وكيفية اكتشافها، وأي وثائق مساندة) وحفظها ومراجعتها دورياً.

٧- عقد اجتماعات لمناقشة "الدروس المستفادة" مع كافة الأطراف المعنية بعد وقوع حادثة كبيرة من أجل دراسة التهديدات الجديدة وتحسين التقنيات المستخدمة والدروس المستفادة كجزء من عملية التعافي.

٨- إطلاع مسؤولي التخطيط لاستمرارية الأعمال على طبيعة الحوادث وتأثيراتها حتى يتمكنوا من تحديد تقييمات الأثر على الأعمال وتقييمات المخاطر وخطط عمليات الاستمرارية بصورة مناسبة.

٩- إشراك مختصي التخطيط لاستمرارية الأعمال في جامعة الملك فيصل من المراحل الأولى من عمليات اكتشاف حوادث الأمن السيبراني والاستجابة لها لتقليل انقطاع الأعمال خلال الظروف الشديدة؛ حيث من الممكن الاستفادة منهم في التخطيط للاستجابة لحالات معينة مثل هجمات تعطيل الشبكات (Denial of Service "DoS").

٩-٥ الحفاظ على المعلومات الاستباقية بشأن التهديدات (Threat Intelligence Feeds Maintenance)

الهدف

ضمان اطلاع جامعة الملك فيصل على التهديدات وجوانب الاستغلال وكيفية توفير الحماية ضد هذه التهديدات بصورة ملائمة، وذلك من خلال تزويدها بمعلومات استباقية حول التهديدات، حيث تشمل هذه المعلومات بيانات منظمة وتحليلات للهجمات الأخيرة والحالية والمحتملة والتي يمكن أن تشكل تهديداً سيبرانياً لجامعة الملك فيصل.

المخاطر المحتملة

يمكن أن يؤدي الإخفاق في اطلاع جامعة الملك فيصل على التهديدات وجوانب الاستغلال بصورة ملائمة إلى مخاطر شديدة قد تتسبب بسرقة المعلومات أو الوصول غير المصرح به لها أو الكشف عنها.

الإجراءات المطلوبة

١- جمع المعلومات عن تهديدات الأمن السيبراني مثل المؤشرات (كعنوان بروتوكول الإنترنت للأوامر المشبوهة، واسم النطاق لنظام أسماء النطاقات، والعنوان "URL" الذي يرتبط بمحتوى خبيث) من مجموعة من المصادر، بما في ذلك مستودعات المصادر المفتوحة والمعلومات الاستباقية عن التهديدات التجارية والشركاء الخارجيين، وتنظيمها في قاعدة بيانات معرفية.

٢- تنظيم وتخزين المؤشرات في قاعدة بيانات معرفية بصيغة حرة مثل قواعد بيانات "Wikis"، وقواعد البيانات المنظمة بهدف تخزين مجموعات المؤشرات وتنظيمها وتتبعها والاستفسار عنها. وتشمل المعلومات المتوفرة في القاعدة المعرفية عموماً ما يلي:

- مصدر المؤشر وتاريخ أو وقت الحصول عليه.
- القواعد التي تحكم استخدام المؤشر أو مشاركته.
- فترة صلاحية المؤشر.
- معلومات حول ما إذا كانت الهجمات المصاحبة للمؤشر قد استهدفت جهات أو قطاعات معينة.
- أي سجلات مصاحبة للمؤشر لتعداد الثغرات الشائعة (CVE)، وتعداد المنصات الشائعة (CPE)، وتعداد نقاط الضعف الشائعة (CWE)، وتعداد الإعدادات الشائعة (CCE).
- المجموعات والجهات المعادية والأسماء الوهمية المصاحبة للمؤشر.
- التكتيكات والأساليب والإجراءات التي تستخدمها الجهات المعادية عموماً.
- دوافع الجهات المعادية أو نواياها.

- الأفراد أو سمات الأفراد المستهدفين بالهجمات المصاحبة.
- الأنظمة المستهدفة بالهجمات.

٣- مشاركة المعلومات المتعلقة بالتهديدات ومؤشرات الانتهاك مع الهيئة الوطنية للأمن السيبراني.

* فئات الآثار على الخدمات Table A – Functional Impact Categories

يتم تصنيف تأثيرات المخاطر على خدمات الجامعة وفقاً للجدول التالي: (جدول رقم: ١١ – فئات الأثار على الخدمات).

الفئة	التعريف
لا يوجد None	لا يوجد تأثير على قدرة جامعة الملك فيصل على تقديم الخدمات لكافة المستخدمين.
منخفض Low	ما زالت جامعة الملك فيصل قادرة على تقديم كافة الخدمات الأساسية لكافة المستخدمين، ولكنها تفتقد إلى الفعالية.
متوسط Medium	لم تعد جامعة الملك فيصل قادرة على تقديم الخدمات الأساسية لمجموعة فرعية من المستخدمين.
مرتفع High	لا تستطيع جامعة الملك فيصل تقديم بعض الخدمات الأساسية لأي من المستخدمين.

* فئات الآثار على المعلومات Table B– Informational Impact Categories

يتم تصنيف تأثيرات المخاطر على معلومات لجامعة وفقاً للجدول التالي: (جدول رقم: ١٢ – فئات الأثار على المعلومات).

الفئة	التعريف
لا يوجد None	لم يتم تسريب المعلومات أو تغييرها أو حذفها، ولم تتعرض لأي انتهاك أمني.
انتهاك الخصوصية Privacy Breach	الوصول إلى المعلومات القابلة لتحديد الشخصية (PII) للعاملين والمستفيدين وغيرهم أو تسريبها.
انتهاك المعلومات المملوكة Proprietary Breach	الوصول إلى المعلومات المملوكة، مثل معلومات البنية التحتية الحساسة المحمية (PCII)، أو تسريبها.
انتهاك سلامة المعلومات	تغيير المعلومات المحمية أو المملوكة أو حذفها.

الفئة	التعريف
Integrity Loss	

* فئات التعافي من آثار الحوادث Table C- Recoverability Effort Categories

يتم تصنيف فئات التعافي من آثار الحوادث السيبرانية وفقاً للجدول التالي: (جدول رقم: ١٣ – فئات التعافي من آثار الحوادث).

الفئة	التعريف
اعتيادي Regular	يمكن التنبؤ بالوقت اللازم للتعافي بالاستعانة بالموارد الحالية.
تكميلي Supplemented	يمكن التنبؤ بالوقت اللازم للتعافي بالاستعانة بموارد إضافية.
ممتد Extended	لا يمكن التنبؤ بالوقت اللازم للتعافي وهناك حاجة إلى موارد إضافية ومساعدة خارجية.
غير قابل للتعافي Not Recoverable	من غير الممكن التعافي من الحادثة (مثل حوادث تسرب بيانات حساسة أو نشرها)، ويجب البدء بالتحقيق فيها.

* تصنيف الحوادث وفقاً لمستوى الحدة Table D – Classification of Incidents Based on Severity Level

يتم تصنيف الحوادث السيبرانية وفقاً لمستوى حدتها كما في الجدول التالي: (جدول رقم: ١٤ – تصنيف الحوادث وفقاً لمستوى الحدة).

مستوى الحدة	الوصف	وقت الاستجابة المستهدف	وقت الحل المستهدف
مرتفع جداً Very High	• تهديد أو أثر مباشر على صورة جامعة الملك فيصل أو سمعتها أو مصداقيتها. • تأثر العديد من وحدات الأعمال الوظيفية بصورة كبيرة. • تأثر موقع الأعمال بصورة كبيرة. • الحاجة إلى تفعيل إجراءات استمرارية الأعمال.	فوري	ساعتان
مرتفع High	انقطاع كبير يؤثر على وحدات الأعمال الوظيفية أو الخدمات الرئيسية أو موقع الجهة	ساعة - ساعتان	٤-٥ ساعات
متوسط Medium	تدهور متوسط في سير عمل وحدات الأعمال الوظيفية أو المواقع أو الأصول التقنية والمعلوماتية، إضافة إلى أثر يتراوح ما بين المتوسط والمرتفع على وحدات الأعمال غير الهامة في جامعة الملك فيصل.	٢-٣ ساعات	٨-٩ ساعات
منخفض Low	• المشكلة صغيرة وعلى نطاق بسيط. • تؤثر المشكلة على عدد قليل من الموارد. • يمكن تحمل المشكلة لفترة زمنية محددة.	٥ ساعات	٢٤ ساعة

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٠. معيار اختبار الاختراق

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لاختبار وتقييم مدى فعالية قدرات تعزيز الأمن السيبراني في جامعة الملك فيصل وذلك من خلال محاكاة تقنيات الهجوم السيبراني وأساليبه الفعلية، واكتشاف نقاط الضعف الأمنية غير المعروفة التي قد تؤدي إلى الاختراق السيبراني لجامعة الملك فيصل من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أنظمة جامعة الملك فيصل الحساسة ومكوناتها التقنية، وجميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية والتي تشمل البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف الذكية واللوحية، والبريد الإلكتروني، والدخول عن بعد، وتنطبق هذه السياسة على جميع العاملين في جامعة الملك فيصل.

المعايير

١٠-١ المتطلبات العامة

الهدف

تحديد المتطلبات العامة لاختبار الاختراق (Penetration Testing) التي يجب أن يتبعها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.

المخاطر المحتملة

يمكن أن يؤدي اختبار الاختراق غير المخطط له بشكل صحيح إلى مخرجات غير كافية أو غير دقيقة، أو قد يؤثر على كفاءة الأنظمة.

الإجراءات المطلوبة

١- يجب تطوير خطة لاختبار الاختراق يوضح فيها نطاق العمل وتاريخ البدء والانتهاء وآلية وسيناريوهات تنفيذ عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية.

٢- يجب التأكد من أن خطة العمل لاختبار الاختراق متوافقة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٣- يجب التأكد من أن اختبار الاختراق يسير وفقاً لمنهجية محددة ووفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٤- يجب صياغة وثيقة قواعد التنفيذ قبل البدء بالاختبار والتي تغطي نطاق الاختبار ومدته والأنظمة المستهدفة والبنود والشروط.

٥- يجب إعداد تقرير لنتائج اختبار الاختراق يوضح تأثير المخاطر وآلية معالجتها والمسؤول عن تطبيقها والفترة الزمنية اللازمة لتنفيذها، على أن يتضمن التقرير الأقسام التالية على الأقل:

- الملخص التنفيذي.
- مقدمة لإعداد التقارير.
- المنهجية المتبعة في تصنيف الثغرات.
- الأصول المستهدفة، وسيناريوهات الهجمات (Attack Scenarios).
- تقرير تفصيلي لنتائج اختبار الاختراق.

٦- بعد الانتهاء من تقرير اختبار الاختراق، يجب إعداد خطة عمل لتنفيذ التوصيات، على أن يتضمن التقرير ما يلي على الأقل:

- المسؤول التقني عن الأصل (Technical Owner).
- مالك الأصل (Business Owner).
- الإجراءات المطلوبة لتنفيذ التوصيات.
- الفترة الزمنية اللازمة لتنفيذ التوصيات.

٧- يجب التأكد من أن تقنيات المستخدمين وأدواتهم وحساباتهم، وكذلك الأجهزة المستخدمة في اختبار الاختراق أو كانت جزءاً منه، خاضعة للتحكم والمراقبة وذلك لضمان استخدامها لغرض اختبار الاختراق فقط.

٨- يجب تعطيل أو إزالة التقنيات والأدوات وحسابات المستخدمين بعد الانتهاء من عملية اختبار الاختراق.

٩- يجب إعداد تقرير لكل اختبار اختراق غير ناجح أو غير مكتمل توضح فيه الصعوبات التي واجهت فريق الاختبار لدراسة العوائق وحلها وإعادة الاختبار مرة أخرى.

٢-١٠ آلية اختبار الاختراق

الهدف

تحديد آلية اختبار الاختراق والأدوات والتقنيات المستخدمة التي يجب أن يتبعها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.

المخاطر المحتملة

يمكن أن يؤدي اختبار الاختراق غير المدروس إلى حصول ثغرات جديدة أو وصول غير مصرح به أو استمرار وجود نقاط ضعف أمنية في البيئة لا يتم اكتشافها مما يؤدي إلى نتائج غير دقيقة، كما يمكن أن يؤدي إلى تسرب البيانات أو كشفها أو إلحاق الضرر بالأنظمة والخدمات والمكونات التقنية.

الإجراءات المطلوبة

١- يجب إجراء اختبار الاختراق دورياً. (ECC-2-11-3-2)

٢- يجب إجراء اختبار الاختراق لجميع الخدمات المقدمة خارجياً ومكوناتها التقنية دورياً وحسب جدول محدد ووفقاً لمنهجية وإجراءات محددة. (ECC-2-11-3-1)

٣- يجب إجراء اختبار الاختراق لجميع الأنظمة الحساسة ومكوناتها التقنية بانتظام وبحسب جدول محدد (كل ٦ أشهر) ووفقاً لمنهجية وإجراءات محددة. (CSCC-2-10-1-1)

٤- يجب التأكد من تنفيذ اختبار الاختراق وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، مع الأخذ بالاعتبار الإرشادات التالية:

٢-٤-١ توفير المتطلبات الخاصة ببدء اختبار الاختراق الواردة في إجراءات اختبار الاختراق.

٢-٤-٢ تحديد آلية الاختبار والتي تتضمن اختبار الصندوق الأسود (اختبار اختراق دون توفير معلومات للجهة التي تجري الاختبار)، واختبار الصندوق الأبيض (اختبار اختراق مع توفير جميع المعلومات للجهة التي تجري الاختبار)، واختبار الصندوق الرمادي (اختبار اختراق مع توفير بعض المعلومات للجهة التي تجري الاختبار).

٢-٤-٣ تحديد الأنظمة أو الخدمات أو المكونات التقنية المستهدفة بالاختبار وأي معلومات أو صلاحيات يجب توفيرها قبل بدء اختبار الاختراق.

٢-٤-٤ الاطلاع على تقارير اختبارات الاختراق السابقة والمستندات المساعدة (إن وجدت) مثل مخططات الشبكة والمعايير التقنية الأمنية واستخدامها كمدخلات لعملية اختبار الاختراق لفهم طبيعة الأعمال للنظام أو التطبيق أو المكون التقني.

٢-٤-٥ التأكد من عمل محاكاة لتقنيات الهجوم السيبراني وأساليبه الفعلية خلال عملية اختبار الاختراق تشمل بحد أدنى ما يلي:

- الهندسة الاجتماعية.
- اختبار الاختراق على مستوى الشبكة.
- اختبار الاختراق على مستوى التطبيق.
- اختبار الاختراق للشبكة اللاسلكية.
- الدخول غير المصرح به.

٢-٤-٦ إنشاء منصة أو بيئة تحاكي الأنظمة أو الخدمات المستهدفة باختبار الاختراق لعمل الاختبار عليها بدلاً من الأنظمة والخدمات الإنتاجية (أي الحقيقية).

٢-٤-٧ توثيق النتائج لكل خطوة من خطوات اختبار الاختراق.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**

- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني**.
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني** وإدارة الأمن السيبراني.

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

II. معيار التشفير

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالتشفير الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. كما يجب أن تتوافق مع المعايير الوطنية للتشفير الصادرة من الهيئة الوطنية للأمن السيبراني كمرجع أساسي بأعلى أولوية لمتطلبات الأمن السيبراني الخاصة بالتشفير.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٨-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الأنظمة والتطبيقات وأجهزة معالجة المعلومات الخاصة بجامعة الملك فيصل، وتنطبق على جميع العاملين في جامعة الملك فيصل.

المعايير

II-I استخدام التشفير (Use of Cryptography)

الهدف

ضمان إدارة التشفير واستخدامه بصورة آمنة وملائمة عند الحاجة.

المخاطر المحتملة

يمكن أن يؤدي عدم استخدام التشفير بصورة ملائمة وعند الضرورة إلى مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.

الإجراءات المطلوبة

١- استخدام شهادات تشفير صحيحة لأمن طبقة النقل (TLS) وذلك لكافة المعلومات المحمية المنقولة أو المستخدمة بين العميل والخادم والخوادم الأخرى.

٢- استخدام شهادات تشفير أمن طبقة النقل (TLS) الصادرة عن جهة إصدار شهادات معترف بها لكافة خدمات الإنتاج في جامعة الملك فيصل.

٣- إعداد متصفحات الإنترنت لتجنب البروتوكولات غير الآمنة (مثل "SSLv3" أو "SSLv2") وخوارزميات التشفير الضعيفة (مثل "DES" أو "MD5").

٤- استخدام القنوات المشفرة لكافة عمليات المصادقة.

٥- ضمان حماية النسخ الاحتياطية بصورة ملائمة عن طريق الأمن المادي والتشفير عند تخزينها ونقلها عبر الشبكة، ويشمل هذا النسخ الاحتياطية عن بعد والخدمات السحابية.

٦- إدارة كافة أجهزة الشبكة باستخدام جلسات مشفرة.

٧- في حال اكتشاف خطأ في المعلومات المستلمة خلال عملية التشفير، وطلب المتلقي أن تكون المعلومات صحيحة بالكامل (على سبيل المثال، عندما لا يكون المتلقي قادراً على متابعة أعماله عند وجود خطأ في المعلومات)، يجب تنفيذ الآتي:

- عدم استخدام المعلومات.
- إعادة إرسال المعلومات بناءً على طلب المتلقي (على أن تكون إعادة إرسالها مقتصرة على عدد محدد من المرات).
- تخزين المعلومات المتعلقة بالحادثة في سجل التدقيق لتحديد مصدر الخطأ لاحقاً.

٢-١١ إدارة مفاتيح التشفير (Cryptographic Key Management)

الهدف

ضمان إدارة مفاتيح التشفير بصورة آمنة خلال دورة إدارة مفاتيح التشفير الكاملة.

المخاطر المحتملة

تنطوي إدارة مفاتيح التشفير غير الآمنة على مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.

الإجراءات المطلوبة

١- يجب إدارة مفاتيح التشفير وفقاً لعمليات إدارة مفاتيح التشفير المعتمدة في جامعة الملك فيصل وإجراءاتها وإرشاداتها، ويشمل ذلك إصدار المفاتيح وتخزينها ونسخها احتياطياً واستعادتها وغيرها من العمليات.

٢- يجب تحديد فئات مفاتيح التشفير وفقاً لتصنيفها (عامة، أو خاصة، أو متماثلة) واستخدامها.

٣- يجب حماية مفاتيح التشفير وفقاً لنوعها.

٤- يجب حماية الخصائص المشتركة لمفاتيح التشفير وفقاً لنوعها.

٥- يجب الحصول على ضمان بشأن صلاحية المفاتيح العامة للتأكد من أن مفاتيح التشفير صحيحة حسابياً، وذلك من خلال إحدى الطرق التالية:

- الحصول على ضمان من الجهة المسؤولة عن المفتاح أو الجهة المسؤولة عن التحقق من المفتاح أو طرف خارجي موثوق.
- التحقق المباشر من المفاتيح العامة اعتماداً على الخوارزميات المستخدمة.

٦- يجب استخدام خوارزميات توفر ضماناً بشأن ملكية المفتاح العام أو الحصول على هذا الضمان مباشرة للتأكد من أن الجهة الخارجية (أي الطرف الخارجي) التي توفر المفتاح العام تملك فعلياً المفتاح الخاص المصاحب للمفتاح العام.

٧- يجب توفير الحماية الأمنية الواردة في الضابط ٢-٢ لفترة زمنية معينة وفقاً لنوع مفتاح التشفير.

٨- يجب تعيين مدة تشفير لمفاتيح التشفير.

٩- يجب إتلاف كافة المفاتيح المتماثلة والمفاتيح الخاصة في نهاية فترة حمايتها كما هو مبين في الضابط ٢-٦.

١٠- يجب استخدام أطوال مفاتيح التشفير التي لا تقل عن ١٢٨ بت في جميع خوارزميات المفاتيح المتماثلة.

١١- يجب استخدام مفاتيح نظام التشفير غير المتماثلة ذات الطول الكافي لكي تكون بنفس درجة قوة أطوال المفاتيح المتماثلة.

١٢- بالنسبة للأنظمة الحساسة، من المستحسن استخدام أطوال مفاتيح تشفير متماثلة لا تقل عن ٢٥٦ بت، وأطوال مفاتيح تشفير غير متماثلة (ECC Elliptic Curve Cryptography) لا تقل عن 512 بت.

٣-II تشفير البيانات والمعلومات (Data and Information Encryption)

الهدف

ضمان تشفير البيانات والمعلومات عند الضرورة.

المخاطر المحتملة

تنطوي البيانات والمعلومات غير المشفرة على مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.

الإجراءات المطلوبة

١- يجب استخدام برنامج تشفير القرص الكامل المعتمد لتشفير القرص الصلب في كافة الأجهزة المحمولة.

٢- يجب فك تشفير كافة أنواع حركة بيانات الشبكة المشفرة عند الخادم الوكيل على حدود الشبكة قبل تحليل المحتوى. ويمكن لجامعة الملك فيصل استخدام قائمة محددة من التطبيقات لمواقع مسموحة يمكن الوصول إليها عبر خادم وكيل دون فك تشفير حركة البيانات.

٣- يجب على كافة عمليات الوصول وتسجيل الدخول عن بعد إلى شبكة الجامعة تشفير البيانات قيد الاستخدام والنقل، واستخدام التحقّق من الهوية متعدّد العناصر.

٤- يجب مراقبة كافة أنواع الحركة التي تخرج من جامعة الملك فيصل وكشف أي استخدام غير مصرح به للتشفير.

٥- إذا كانت أجهزة التخزين (USB) مطلوبة، يجب تشفير البيانات المخزنة بناءً على تصنيفها على هذه الأجهزة.

٦- يجب تشفير جميع المعلومات المحمية أثناء الاستخدام والنقل.

٧- يجب تشفير جميع المعلومات المحمية أثناء التخزين باستخدام أداة تتطلب آلية تحقق ثانوية غير مدمجة في نظام التشغيل من أجل الوصول إلى المعلومات.

٨- يجب تشفير جميع البيانات اللاسلكية أثناء الاستخدام والنقل.

٩- يجب تشفير أو اختزال كافة بيانات الاعتماد باستخدام بيانات عشوائية عند تخزينها.

١٠- يجب ضمان أن جميع أسماء المستخدمين وبيانات التحقق الخاصة بالحسابات تُنقل عبر الشبكات باستخدام قنوات مشفرة.

٤-II المعلومات الأخرى ذات العلاقة بالتشفير (Other Cryptographic Related Information)

الهدف

ضمان إدارة البيانات والمعلومات المستخدمة مع مفاتيح التشفير بصورة آمنة.

المخاطر المحتملة

قد تؤدي الإدارة غير الآمنة للبيانات والمعلومات المستخدمة مع مفاتيح التشفير إلى مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.

الإجراءات المطلوبة

١- يجب حماية كافة المعلومات المستخدمة مع خوارزميات التشفير ومفاتيح التشفير.

٢- يجب حماية الخصائص المشتركة لمعلومات التشفير وفقاً لنوعها.

٣- يجب الحصول على ضمان بشأن صلاحية "معيار النطاق" لكافة خوارزميات المفاتيح العامة الخاصة بالدخول المنفصل لضمان صحة معايير النطاق حسابياً. وذلك من خلال إحدى الطرق التالية:

- الحصول على ضمان من الجهة المسؤولة عن المفتاح أو الجهة المسؤولة عن التحقق من المفتاح أو طرف خارجي موثوق.
- التحقق من المفاتيح العامة اعتماداً على الخوارزميات المستخدمة.

٤- يجب توفير الحماية الأمنية الواردة في الضابط ٢-٢ لفترة زمنية معينة وفقاً لنوع معلومات التشفير.

٥- يجب إدراج آليات لا تعتمد على التشفير في أنظمة الاتصالات لضمان توافر المعلومات المشفرة المنقولة بعد استلامها بنجاح، بدلاً من الاعتماد على إعادة إرسالها من قبل المرسل الأصلي لغايات توافرها مستقبلاً.

٥-II بروتوكولات التشفير وخوارزميات التشفير المدعومة (Encryption Protocols and Cipher Suites)

الهدف

ضمان استخدام خوارزميات التشفير المعتمدة والآمنة عند التشفير.

المخاطر المحتملة

ينطوي استخدام خوارزميات التشفير غير الآمنة أو غير المعتمدة على مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.

الإجراءات المطلوبة

١- يجب استخدام خوارزميات دوال الاختزال المشفرة فقط بحيث لا يكون من الممكن العثور على نص له نتيجة اختزال معينة (مقاومة عكس الخوارزمية)، أو العثور على نصين لهما نفس نتيجة الاختزال (مقاومة التصادم).

٢- يجب استخدام خوارزميات دوال اختزال مشفرة وفقاً لمعايير الخوارزميات ذات العلاقة.

٣- يجب استخدام أطوال مفاتيح التشفير التي لا تقل عن ١٢٨ بت في جميع خوارزميات المفاتيح المتماثلة.

٤- يجب استخدام شفرة التحقق من الرسائل (MAC) لضمان سلامة البيانات والتأكد من قيام الجهة المتوقعة بحساب شفرة التحقق من الرسائل (MAC).

٥- يجب استخدام خوارزميات شفرة التحقق من الرسائل (MAC) بناءً على خوارزميات التشفير الكتلي (Block Cipher)، (مثل شفرة التحقق من الرسائل باستخدام التشفير "CMAC" أو شفرة غاليوس للتحقق من الرسائل "GMAC")، أو بناءً على خوارزميات حساب ملخص النص المميز (شفرة التحقق من الرسائل المجزأة "HMAC").

٦- يجب عدم استخدام نفس المفتاح لغايات التشفير واحتساب شفرة التحقق من الرسائل (MAC) في حال استخدام نفس خوارزمية التشفير الكتلي (Block Cipher).

٧- يجب استخدام خوارزميات التواقيع الرقمية المعتمدة لتوفير التحقق الآمن والتحقق من سلامة المعلومات ودعم عدم إنكار صحة البيانات.

٨- يجب استخدام خوارزميات التواقيع الرقمية التالية مع أطوال المفاتيح المعتمدة لكل من:

- خوارزمية التوقيع الرقمي (خوارزمية "DSA").
- خوارزمية ريفست وشامير وإديلمان (خوارزمية "RSA").
- خوارزمية التوقيع الرقمي للمنحنى الإهليجي (خوارزمية "ECDSA").

٩- يجب إصدار التواقيع الرقمية باستخدام مفاتيح تلبي أو تتجاوز أطوال المفاتيح المعتمدة للخوارزمية.

١٠- يجب استخدام طرق تبادل المفاتيح المعتمدة التالية لإعداد المفاتيح بين الجهات التي تقوم بالاتصالات:

- نقل المفاتيح: يجب نقل مواد صياغة المفاتيح من جهة إلى أخرى باستخدام خوارزمية متماثلة (أي باستخدام مفاتيح تشفير المفاتيح) أو باستخدام خوارزمية غير متماثلة.
- الاتفاق على المفاتيح: يجب أن تتعاون الجهات في إنشاء مواد صياغة المفاتيح المشتركة باستخدام خوارزميات متماثلة أو غير متماثلة.

١١- يجب استخدام طرق تبادل المفاتيح المعتمدة باستخدام أطوال المفاتيح المعتمدة. وتشمل هذه الطرق خوارزمية ديفي- هيلمان (خوارزمية "DH") وخوارزمية "RSA".

١٢- يجب استخدام درجة قوة لا تقل عن ٢٥٦ بت لخوارزميات التشفير المستخدمة للأنظمة الحساسة حسب ما تصدره الهيئة الوطنية للأمن السيبراني في هذا الخصوص.

١٣- يجب استخدام درجات قوة لا تقل عن ٢٥٦ بت لخوارزميات حساب ملخص النص المميز المستخدمة للأنظمة الحساسة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٢. معيار حماية تطبيقات الويب

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية تطبيقات الويب الخارجية الخاصة بجامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-١٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع تطبيقات الويب الخارجية الخاصة بجامعة الملك فيصل، وينطبق على جميع العاملين في جامعة الملك فيصل.

المعايير

١-١٢ إدارة هويات الدخول (Access Management)

الهدف

ضمان حماية تطبيقات الويب من الوصول غير المصرح به.

المخاطر المحتملة

يترتب على الوصول غير المصرّح به لتطبيقات الويب مخاطر كبيرة قد تؤدي إلى تسرب أو سرقة المعلومات، وقد تساعد هذه المعلومات في تنفيذ المزيد من الهجمات السيبرانية ضد البنية التحتية لجامعة الملك فيصل.

الإجراءات المطلوبة

١- استخدام مبدأ الحد الأدنى من الصلاحيات والامتيازات "Principle of Least Privilege" الذي يمنح المستخدمين الحد الأدنى من صلاحيات الوصول إلى تطبيقات الويب الخارجية.

٢- حصر الوصول إلى المكونات التقنية الخاصة بالويب وتطبيقات الويب حسب الأدوار الوظيفية (مثل: مشرفو النظام، ومسؤولو دعم التطبيقات، وغيرها) وذلك باستخدام الحسابات الفردية لتلك الأدوار فقط. بالإضافة إلى ذلك، استخدام قوائم التحكم بالوصول إلى الشبكة (ACL) التي تعتمد على عناوين بروتوكولات الإنترنت (IP Address) الخاصة بأجهزة المستخدمين.

٣- إيقاف أو حذف الحسابات الافتراضية غير المستخدمة.

٤- إلى جانب ضرورة إدخال اسم المستخدم وكلمة المرور، إلزام المستخدم باستعمال التحقّق من الهوية متعدّد العناصر باستخدام آليات أخرى للتحقّق من الهوية مثل الخصائص الحيوية والمفاتيح المادية وكلمات المرور المؤقتة والبطاقات الذكية وشهادات التشفير، وغيرها.

٥- استخدام كلمة مرور معقدة للدخول إلى تطبيقات الويب وفقاً لسياسة إدارة هويات الدخول والصلاحيات في جامعة الملك فيصل.

٦- ضبط إعدادات تطبيقات الويب الخاصة بالأنظمة الحساسة من خلال تحديد وقت انتهاء مهلة الجلسة وإقفالها عند عدم الاستخدام (على سبيل المثال، لمدة ٥ دقائق).

٢-١٢ هندسة تطبيقات الويب (Web Application Architecture)

الهدف

تحديد متطلبات الأمن السيبراني في بناء تطبيقات الويب وتصميمها وتطبيقها بشكل آمن وفعال.

المخاطر المحتملة

قد يسبب البناء العشوائي لتطبيقات الويب مخاطر أمنية حساسة يمكن استغلالها في الهجمات السيبرانية التي قد تؤثر على أعمال جامعة الملك فيصل.

الإجراءات المطلوبة

١- تنفيذ البنية التحتية لتطبيقات الويب للأنظمة الحساسة باستخدام مبدأ البنية متعددة الطبقات (٣ مستويات على الأقل)، أو معمارية الخدمات الصغيرة المحمية بجدار حماية ثنائي الطبقة. وتحديداً، إدراج خادم الويب في منطقة الإنترنت المحايدة، وخوادم تطبيقات الويب في منطقة الإنتاج، وخوادم قواعد البيانات في المنطقة الموثوقة أو منطقة قاعدة البيانات.

٢- تطبيق العزل المادي أو المنطقي لتطبيقات الويب الحساسة عن التطبيقات أو الأنظمة الأخرى. فعلى سبيل المثال، يمكن تحقيق العزل المادي من خلال استضافة تطبيقات الويب في بيئة مادية منفصلة ومختلفة تماماً، في حين يمكن تحقيق العزل المنطقي من خلال إدراج تطبيقات الويب في مناطق منفصلة داخل الشبكة دون السماح بالوصول إليها من أي منطقة أخرى.

٣- عزل تطبيقات الويب الخاصة بالإنتاج منطقياً عن بيئة الاختبار وبيئة التطوير باستخدام محددات الشبكة عن طريق ضبط إعدادات قوائم التحكّم بالوصول (ACL) والسياسات الأمنية على جدران الحماية.

٤- تقييد الوصول عبر الشبكة لتطبيقات الويب وحصره بمنطقة خوادم الويب، ومنطقة خوادم تطبيقات الويب، ومنطقة الإدارة.

٥- تثبيت جدار الحماية لتطبيقات الويب (WAF) على خوادم تطبيقات الويب للتحقق من حركة البيانات الواردة والمصادقة عليها، وتسجيل أي حركة بيانات غير مصرح بها وحجبها، حيث تعمل أجهزة جدار الحماية لتطبيقات الويب (WAF)على كشف هجمات الويب أو هجمات التطبيقات على الخدمات الخارجية وتطبيقات الويب أو حجبها. (بالإضافة إلى ذلك، إعداد جدار الحماية لتطبيقات الويب (WAF) لتمكين خاصية التحكم ببروتوكول الإنترنت وخصائص الموقع الجغرافي لبروتوكول الإنترنت من أجل حجب بروتوكولات الإنترنت المحظورة ودول معينة).

٦- إعداد جدار الحماية لتطبيقات الويب (WAF) للحد من أعلى المخاطر الشائعة التي تستهدف تطبيقات الويب الصادرة عن المشروع المفتوح لأمن تطبيقات الويب (OWASP Top Ten) على تطبيقات الويب الحساسة وفقاً للمعايير والإجراءات ذات العلاقة في جامعة الملك فيصل.

٧- ضبط إعدادات نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات (IPS) وجدار الحماية لتطبيقات الويب (WAF) لإتاحة التواقيع التي تطابق سلوك وبروتوكولات تطبيقات الويب (مثل Oracle OHS، وIIS، وApache، وSQL، وXML، وغيرها).

٨- ضبط إعدادات تقنيات الحماية من البرمجيات الضارة وأنظمة الحماية من التهديدات المتقدمة المستمرة للتحقق من كافة عمليات نقل الملفات المرتبطة بتطبيقات الويب بحثاً عن أي ملفات خبيثة وفقاً لسياسة ومعيار الحماية من البرمجيات الضارة المعتمدين في جامعة الملك فيصل.

٩- ضبط إعدادات تقنيات وأنظمة حماية تطبيقات الويب لتتبع نموذجاً أمنياً إيجابياً أو نموذج السماح بقائمة محددة من التطبيقات، وذلك من خلال السماح بأنواع محددة من عمليات نقل الملفات، وبروتوكولات ومنافذ محددة، وتطبيقات ويب محددة من المستوى ٧، ومتغيرات تطبيقات ويب محددة، وحجب جميع التطبيقات والملفات التي لم يتم ضبط إعداداتها.

١٠- استخدام تطبيقات ويب وبروتوكولات اتصالات آمنة مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وبروتوكول أمن طبقة النقل (TLS) وغيرها.

١٢-٣ مراجعة الإعدادات والتحصين (Secure Configuration and Hardening)

الهدف

تحديد الإعدادات والتحصين ومراجعتها للتأكد من ضبط إعدادات تطبيقات الويب وتشغيلها بشكل آمن وفعال.

المخاطر المحتملة

قد يؤدي عدم الدقة في ضبط إعدادات تطبيقات الويب ومكوناتها التقنية إلى ظهور ثغرات أمنية يمكن استغلالها لشن هجمات سيبرانية أو التأثير على سير الأعمال في جامعة الملك فيصل.

الإجراءات المطلوبة

١- يجب إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسات إدارة الثغرات الأمنية واختبار الاختراق المعتمدة في جامعة الملك فيصل.

٢- إجراء اختبارات دورية لتقييم حماية تطبيقات الويب مثل اختبار أمن التطبيقات الثابت (SAST) واختبار أمن التطبيقات الديناميكي (DAST).

٣- تنصيب حزم التحديثات والإصلاحات على تطبيقات الويب ومكوناتها التقنية بانتظام وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في جامعة الملك فيصل.

٤- إيقاف الوظائف والخدمات وملفات الإعدادات غير الضرورية أو غير المستخدمة أو تعطيلها.

٥- حجب إمكانية الوصول إلى الملفات والمجلدات المشاركة عبر الشبكة غير الضرورية أو غير اللازمة.

٦- حماية الشفرة المصدرية وتحصينها.

٧- إنشاء نسخ أو قوالب آمنة لكافة تطبيقات الويب بناءً على المعايير الأمنية المعتمدة. وإعادة نسخ تطبيقات الويب باستخدام أحد قوالب النسخ في حال تعرضها لانتهاك أمني.

٨- تخزين النسخ في بيئة آمنة على خوادم مؤمنة والتحقق منها باستخدام أدوات مراقبة سلامة المعلومات دورياً.

٩- يجب مزامنة توقيت تطبيقات الويب من مصادر الوقت المعتمدة من قبل جامعة الملك فيصل.

١٢-٤ توافر المعلومات (Availability)

الهدف

الحفاظ على توافر تطبيقات الويب الخارجية وحمايتها من هجمات حجب الخدمة (DoS Attacks) وتعطل الخدمة العرضي.

المخاطر المحتملة

إذا لم يتم توفير أنظمة الحماية من هجمات حجب الخدمة وتعطل البنية التحتية، قد تكون تطبيقات الويب هدفاً لهجمات حجب الخدمة، مما قد يسبب انقطاعاً دائماً في الخدمات أو يؤثر على كفاءة تطبيق الويب.

الإجراءات المطلوبة

١- استخدام مبدأ معمارية تطبيقات الويب التوزيعية الذي يعمل على توزيع نقاط التعطل الحاسمة.

٢- توفير تقنيات توزيع الجهد (Load Balancer) مثل تقنيات توزيع حركة البيانات والاتصالات.

٣- تطبيق آليات تكرار البيانات (Data Replication) على تطبيقات الويب في مواقع التعافي من الكوارث أو المواقع البديلة (Secondary Data Center).

٤- توفير نسخة مطابقة لبيئة إنتاج تطبيقات الويب للأنظمة الحساسة في موقع التعافي من الكوارث.

٥- فيما يتعلق بتطبيقات الويب التي تستضيفها أطراف خارجية، يجب أن تتضمن بنود اتفاقية مستوى الخدمة مستوى مقبول من توافر تطبيقات الويب والخدمات المقدمة من خلالها، وفقاً لسياسة الأمن السيبراني المتعلق بالأطراف الخارجية المعتمدة في جامعة الملك فيصل.

٦- ضبط إعدادات إعادة توجيه حركة بيانات تطبيقات الويب تلقائياً أو يدوياً لموقع النسخ الاحتياطية أو التعافي من الكوارث في حال تعطل بيئة الإنتاج.

١٢-٥ التشفير (Cryptography)

الهدف

ضمان سرية بيانات تطبيقات الويب والتأكد من سلامتها.

المخاطر المحتملة

في حال عدم استخدام تقنيات التشفير والتحقق من سلامة المعلومات، يمكن أن تتعرض المعلومات المحمية وبيانات تطبيقات الويب إلى الكشف أو التلاعب بها أو الوصول غير المصرح به.

الإجراءات المطلوبة

١- تطبيق تقنيات التشفير مثل أمن طبقة النقل (Transport Layer Security) والشبكات الخاصة الافتراضية (Virtual Private Networks) لحماية تقنيات التحقّق من الهوية (Authentication)، إلى جانب استخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) وفقاً لمعيار التشفير المعتمد في جامعة الملك فيصل.

٢- ضبط إعدادات تطبيقات الويب وتمكينها من استخدام بروتوكولات آمنة للتشفير حيثما أمكن، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول النقل الآمن (FTP) عبر أمن طبقة النقل (TLS) وغيرها.

٣- توفير تقنيات التشفير للاتصالات بين الخوادم وأجهزة المستخدمين في تطبيقات الويب (End-to-End Encryption).

٤- تقييد استخدام بروتوكولات النقل الآمن (SSHv2) وبروتوكول التحكم بسطح المكتب عن بعد (RDP) عن طريق تقنيات التشفير مثل أمن طبقة النقل (TLS).

٥- استخدام تقنيات التشفير غير التماثلي القائم على شهادات التشفير (الخاص/العام) لكافة تطبيقات الويب العامة والخارجية وفقاً لمعيار التشفير المعتمد في جامعة الملك فيصل.

٦- شراء شهادات تشفير تطبيقات الويب من جهة إصدار شهادات موثوقة ومعتمدة وفقاً للمتطلبات التنظيمية والتشريعية ذات العلاقة والتأكّد من تجديدها بشكل دوري.

٧- تثبيت وظائف التشفير وإدارة شهادات التشفير على جدار الحماية لتطبيقات الويب للسيطرة بشكل أكبر على الهجمات والتهديدات.

٨- تخزين مفاتيح تشفير تطبيقات الويب في مكان ملائم وآمن وفقاً للسياسات والإجراءات ذات العلاقة في جامعة الملك فيصل.

١٢-٦ تسجيل الأحداث وسجل التدقيق (Event and Audit Logging)

الهدف

ضمان حفظ سجلات الأحداث لتطبيقات الويب في جامعة الملك فيصل ومراقبتها.

المخاطر المحتملة

يؤدي عدم حفظ ومراقبة سجلات الأحداث لتطبيقات الويب في جامعة الملك فيصل إلى صعوبة الكشف عن حوادث وتهديدات الأمن السيبراني وغيرها، وقد يتسبب بمضاعفة الأضرار التي قد تلحق بالتطبيقات.

الإجراءات المطلوبة

١- تفعيل جميع سجلات الأحداث (سجلات التدقيق والسجلات المتعلقة بالأمن السيبراني) لجميع تطبيقات الويب ومكوناتها التقنية.

٢- جمع سجلات الأحداث الخاصة بالأمن السيبراني في نظام تسجيل مركزي (SIEM) وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدين في جامعة الملك فيصل.

١٢-٧ النسخ الاحتياطي والأرشفة (Backup and Archival)

الهدف

ضمان سلامة بيانات تطبيقات الويب من العبث بها أو فقدانها بالخطأ أو تخريبها، والتأكد من توافرها وقابلية استعادتها.

المخاطر المحتملة

في حال حذف بيانات تطبيقات الويب أو العبث بها أو فقدانها بالخطأ أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن جامعة الملك فيصل من استرداد البيانات مما سيؤثّر على أنشطة أعمالها الاعتيادية.

الإجراءات المطلوبة

١- عمل نسخ احتياطية كاملة لتطبيقات الويب وترقيمها تسلسلياً وتحديد تاريخها ووقتها وفهرستها وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة الملك فيصل. وينبغي أن تشمل النسخ الاحتياطية على الأقل النسخ الاحتياطية لإعدادات تطبيقات الويب وبيانات ومعلومات تطبيقات الويب المخزنة.

٢- تشفير النسخ الاحتياطية لتطبيقات الويب الخاصة بجامعة الملك فيصل.

٣- تخزين النسخ الاحتياطية من تطبيقات الويب للأنظمة الحساسة الخاصة بجامعة الملك فيصل على الأقل في موقعين ماديين ومعزولين مادياً عن بعضهما البعض.

٤- اختبار إمكانية استرجاع النسخة الاحتياطية كل ثلاثة أشهر أو وفقاً للسياسات والإجراءات ذات العلاقة في جامعة الملك فيصل.

٥- استخدام تقنيات توثيق وسلامة النسخ الاحتياطي لضمان نسخ بيانات تطبيقات الويب وأرشفتها بطريقة صحيحة.

٦- أرشفة النسخ الاحتياطية لتطبيقات الويب الخاصة بجامعة الملك فيصل في موقع تخزين معزول مادياً ومنطقياً ووفقاً للسياسات والإجراءات ذات العلاقة في جامعة الملك فيصل.

٨-١٢ تطبيقات الويب الحديثة والسحابية الأصلية (Modernized and Cloud Native Web Applications)

الهدف

تحديد متطلبات الأمن السيبراني لتطبيقات الويب المستضافة بالحوسبة السحابية لضمان إعدادها وتثبيتها وتشغيلها بطريقة آمنة.

المخاطر المحتملة

قد يؤدي استخدام خدمة الحوسبة السحابية لتشغيل تطبيقات الويب بدون وضع معايير أمنية وتطبيق متطلبات الأمن السيبراني إلى ظهور ثغرات أمنية شائعة يمكن استغلالها لشن هجمات سيبرانية أو التأثير على كفاءة أعمال جامعة الملك فيصل.

الإجراءات المطلوبة

١- تطوير منهجية التطوير الآمن وفقاً لآلية "DevSecOps".

٢- تطوير نظام التكامل المستمر/التثبيت المستمر (CI/CD) الآمن وتطبيقه باتباع أفضل الممارسات.

٣- تنصيب منصة أمن الحاويات من مورد موثوق لإدارة أمن الحاويات وضمان حماية نظام الحاويات.

٤- تنصيب حزم التحديثات والإصلاحات دورياً.

٥- توفير حلول إدارة المعلومات الحساسة وذلك من أجل إدارة المعلومات الحساسة والمفاتيح والشهادات ومنع تخزين المعلومات الحساسة في الحاويات.

٦- استخدام نسخ الحاويات من مصادر موثوقة أو معتمدة.

٧- عزل البنية التحتية الخاصة بالحاويات.

٨- استخدام كشف الثغرات التلقائي لفحص الحاويات قبل وبعد تثبيتها في بيئة الإنتاج.

٩- توفير تقنيات وأدوات المراقبة للتأكد من سلامة تطبيقات الويب وتوافرها وكفاءتها باستمرار.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

١٣. معيار التطوير الآمن للتطبيقات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتطوير البرمجيات والتطبيقات وحمايتها من التهديدات الداخلية والخارجية في جامعة الملك فيصل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ١-٦-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)، ولمزيد من التفاصيل يمكن الرجوع إلى القسم الرابع - قاموس المصطلحات في نهاية هذه الوثيقة.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار كافة أنشطة ومشاريع وممارسات تطوير البرمجيات والتطبيقات والأصول المعلوماتية والتقنية الخاصة بها في جامعة الملك فيصل، وتنطبق على جميع العاملين في جامعة الملك فيصل.

المعايير

١-١٣ التطوير الآمن للتطبيقات (Secure Code Development)

الهدف

توفير متطلبات الأمن السيبراني لضمان حماية أنشطة تطوير البرمجيات والتطبيقات وضوابط الأمن السيبراني لحماية البرمجيات التي يتم تطويرها.

المخاطر المحتملة

يمكن أن يؤدي تطوير التطبيقات غير الآمن إلى إيجاد ثغرات أمنية يمكن استغلالها لتهديد سرية بيانات جامعة الملك فيصل وسلامتها وتوافرها، والتأثير في سير عملها.

الإجراءات المطلوبة

١- تطوير عملية دورة حياة تطوير البرمجيات الآمنة (SSDLC) وتطبيقها.

٢- تطوير منهجية وعملية "التطوير والأمن والعمليات" (DevSecOps) واتباعها.

٣- ضمان توفير متطلبات الأمن السيبراني في المراحل الأولية من تطوير البرمجيات ودمجها في دورة حياة تطوير البرمجيات الآمنة (SSDLC).

٤- ضمان اختبار الأمن السيبراني في مراحل اختبار تطوير البرمجيات ودمجه في دورة حياة تطوير البرمجيات الآمنة (SSDLC).

٥- تصميم وإعداد بيئة آمنة لغايات التطوير والاختبار وضمان الجودة.

٦- تطبيق إرشادات التطوير الآمن للتطبيقات.

٧- تطبيق إجراءات التخفيف على أعلى ١٠ مخاطر تهدد أمن تطبيقات الويب وفقاً للمشروع المفتوح لأمن تطبيقات الويب (OWASP) فيما يخص الأنظمة والتطبيقات الحساسة.

٨- تطبيق آليات لتقييد صلاحيات التعديل على الشفرة المصدرية أو بيانات بيئات الإنتاج.

٩- إلزام الموردين الخارجيين بالالتزام بسياسات ومعايير الأمن السيبراني المعتمدة في جامعة الملك فيصل.

١٠- الحصول على يجب استخدام المصادر الحديثة والموثوق بها والمرخصة فقط لأدوات تطوير البرمجيات والمكتبات والمكونات

١١- ضمان تطبيق ضوابط حماية تطبيقات الويب وفقاً لسياسة ومعيار حماية تطبيقات الويب المعتمدين في جامعة الملك فيصل.

١٢- استخدام خوارزميات تشفير موحدة ومراجعة بدقة وفقاً للمعايير والإجراءات ذات العلاقة.

١٣- التحقق من أن إصدارات كافة البرمجيات التي تم شراؤها من خارج جامعة الملك فيصل مدعومة من المطور ومحصنة بصورة ملائمة بناءً على التوصيات الأمنية للمطور.

١٤- تدريب جميع العاملين في تطوير البرمجيات على كتابة الشفرات المصدرية المناسبة للغة البرمجة وبيئة التطوير المستخدمة.

٢-١٣ مستودع الشفرة المصدرية (Source Code Repository)

الهدف

توفير ضوابط الأمن السيبراني لضمان حماية الشفرة المصدرية والمكتبات ومستودع الشفرة المصدرية.

المخاطر المحتملة

في حال عدم توفير حماية كافية ومناسبة للشفرة المصدرية والمكتبات، يمكن أن تتعرض الشفرة المصدرية في جامعة الملك فيصل للخطر أو يتم التلاعب بها أو الوصول غير المصرح به لها.

الإجراءات المطلوبة

١- استخدام مستودع شفرة مصدرية آمن يمتاز بتطبيق إجراءات التحقق من الهوية والإصدار والرقابة وتسجيل الدخول.

٢- تطبيق إجراءات منع وصول أي شخص إلى الشفرة المصدرية ومستودع الشفرة المصدرية باستثناء مطوري التطبيقات والجهات المسؤولة عنها.

٣- استخدام خطة ترقيم موحدة لضوابط الإصدار بحيث تبين تاريخ تثبيت الإصدارات المحدثة من البرمجيات.

٤- أرشفة الإصدارات القديمة من الشفرة المصدرية دورياً.

٥- فصل الشفرة المصدرية للتطبيقات قيد التطوير عن الشفرة المصدرية للتطبيقات في بيئة الإنتاج.

٦- أرشفة الشفرة المصدرية للتطبيقات التي انتهت صلاحيتها بحيث يمكن استرجاعها عند الحاجة.

٧- الحصول على نسخة من الشفرة المصدرية لكافة التطبيقات التي طورتها أطراف خارجية لجامعة الملك فيصل وتخزينها في مستودع الشفرة المصدرية.

٨- تطوير معايير تحصين وأمن الحاويات والنسخ الافتراضية للنظام (Docker) وإرشادات الممارسات الأمنية المثلى وتطبيقها.

٩- تثبيت آليات إدارة الأسرار وذلك من أجل إدارة الأسرار والمفاتيح والشهادات ومنع تخزين الأسرار في الحاويات.

١٠- استخدام نسخ الحاويات من مصادر موثوقة أو معتمدة.

١١- استخدام سجل حاويات خاص لضمان تنزيل نسخ الحاويات المعتمدة والآمنة فقط على النظام بحيث يمكن فحص كل نسخة بحثاً عن الثغرات المعروفة والشائعة.

١٢- عدم إدارة الحاويات من خلال حسابات المستخدمين عالية الصلاحية والامتيازات.

٣-١٣ مراجعة واختبار الشفرة المصدرية (Secure Code Review and Testing)

الهدف

توفير ضمان بشأن تطبيق ضوابط الأمن السيبراني على تطوير التطبيقات الآمن وكشف نقاط الضعف والثغرات والمشكلات في البرمجيات.

المخاطر المحتملة

يمكن أن تتعرض جامعة الملك فيصل إلى مخاطر أمنية كبيرة في حال عدم اختبار الشفرة المصدرية وأنشطة تطوير الشفرات ومراجعتها بانتظام لغايات الكشف عن الثغرات الأمنية والإعدادات الخاطئة ونقاط الضعف، يمكن أن تتعرض جامعة الملك فيصل إلى مخاطر أمنية كبيرة.

الإجراءات المطلوبة

١- إجراء عملية مراجعة الشفرة المصدرية بانتظام لتطبيقات الويب المطورة داخلياً.

٢- تطبيق أدوات التحليل الثابتة والديناميكية للتحقق من الالتزام بممارسات تطوير التطبيقات الآمن بالنسبة للبرمجيات المطورة داخلياً.

٣- القيام بمراجعة أمنية الشفرة المصدرية بانتظام لكافة التطبيقات المطورة لجامعة الملك فيصل من قبل أطراف خارجية.

٤- مراجعة واعتماد الضوابط الأمنية للتطبيقات المطورة داخلياً قبل تثبيتها في بيئة الإنتاج.

٥- إعادة تقييم التطبيقات الحالية المطورة داخلياً وإعادة اعتمادها بعد إجراء تغيير رئيسي عليها أو بعد مرور فترة زمنية محددة.

٦- إجراء تقييم المخاطر لكافة التطبيقات قيد التطوير أو التي يتم شراؤها لتحديد الضوابط المطلوبة لتقليل مخاطر التطبيقات إلى مستويات مقبولة قبل التثبيت في بيئة الإنتاج (يرجى الرجوع إلى سياسة إدارة المخاطر المعتمدة في جامعة الملك فيصل).

٧- إجراء اختبار الالتزام بالأمن السيبراني للبرمجيات بناءً على سياسات الأمن السيبراني المعتمدة في جامعة الملك فيصل قبل التثبيت في بيئة الإنتاج.

٨- استخدام معيار التحقق من حماية التطبيقات الصادر عن المشروع المفتوح لأمن تطبيقات الويب (OWASP) كدليل إرشادي لتحديد المتطلبات الأمنية وعمل حالات اختبار لمراجعة الأنظمة والتطبيقات الحساسة.

٩- إجراء مراجعة لإعدادات البرمجيات بما في ذلك مراجعة الإعدادات والتحصين وحزم التحديثات قبل التثبيت في بيئة الإنتاج.

١٠- إجراء اختبارات الأمن السيبراني، بما في ذلك تقييم الثغرات واختبار الاختراق ومراجعة تطوير التطبيقات الآمن، قبل التثبيت في بيئة الإنتاج.

١١- إجراء اختبارات الأمن السيبراني، بما في ذلك تقييم الثغرات واختبار الاختراق، بعد التثبيت في بيئة الإنتاج.

١٢- معالجة كافة المشاكل الأمنية في التطبيقات المطورة التي يتم اكتشافها خلال مراجعة تطوير التطبيقات الآمن قبل التثبيت في بيئة الإنتاج.

١٣- اختبار التطبيقات المطورة لضمان تطبيق ضوابط فصل المهام بالصورة الملائمة.

١٤- إلغاء حسابات الاختبار الموجودة في بيئة غير بيئة الإنتاج قبل نقل التطبيقات إلى بيئة الإنتاج.

١٥- فصل بيئة الاختبار والتطوير منطقياً عن بيئة الإنتاج والبيئات الأخرى باستخدام محددات الشبكة عن طريق إعداد وتثبيت قوائم التحكّم بالوصول (ACL) والسياسات الأمنية على جدران الحماية.

١٦- إجراء مراجعة النظير للشفرة المصدرية من قبل مطور لم يشارك في كتابة أي شفرة قبل التثبيت في بيئة الإنتاج في جامعة الملك فيصل.

١٧- استخدام الشفرة المصدرية وأدوات تقييم أمن البرمجيات المعتمدة والمرخصة.

١٨- إجراء الاختبارات الأمنية للتطبيقات المطورة في كافة مراحل اختبار دورة حياة تطوير البرمجيات (SDLC)، بما في ذلك الاختبارات غير الوظيفية، واختبار الوحدات (UT) واختبار تكامل الأنظمة (SIT)، واختبار قبول المستخدم (UAT).

١٩- استحداث عملية لإدارة العيوب البرمجية في البرمجيات والثغرات والمشكلات الأمنية ووضع سجل خاص بها ومتابعتهما.

٢٠- إدراج الاختبارات كجزء من عمليات التحسين المستمر والتطوير المستمر (CI/CD).

٤-١٣ إرشادات التطوير الآمن للتطبيقات

يشتمل الجدول التالي: (جدول رقم: ١٥- إرشادات التطوير الآمن للتطبيقات) على عمليات التحقق من الهوية وإجراءات التحقق من الهوية غير الآمنة.

١	عمليات التحقق من الهوية (OWASP:A2:2017 - إجراءات التحقق من الهوية غير الآمنة) Authentication (OWASP:A2:2017 – Broken Authentication)
١-١	التحقق من أن كافة الصفحات والمصادر تقتضي التحقق من الهوية باستثناء المحددة خصوصاً لتكون عامة (مبدأ التحقق التام والمتكامل).
١-٢	التحقق من أن حقول كلمات المرور لا تُظهر كلمات مرور المستخدمين عند إدخالها وأن خاصية الإكمال التلقائي في حقول كلمات المرور (أو الأشكال التي تتضمنها) غير مفعلة.
١-٣	التحقق من أن كافة ضوابط التحقق من الهوية تخفق بصورة آمنة لضمان عدم قدرة الجهات المهاجمة على تسجيل الدخول.
١-٤	التحقق من أن بيانات الاعتماد وكافة معلومات الهوية الأخرى التي يتعامل معها التطبيق لا تمر عبر روابط غير مشفرة أو مشفرة بصورة غير آمنة.
١-٥	التحقق من أن مسار "نسيت كلمة المرور" ومسارات الاستعادة الأخرى لا ترسل كلمات المرور الحالية أو الجديدة من غير تشفير.
١-٦	التحقق من أن تنفيذ هجمات تعداد اسم المستخدم (User Enumeration) غير ممكن عن طريق وظائف "تسجيل الدخول" أو "إعادة ضبط كلمة المرور" أو "نسيت الحساب".
١-٧	التحقق من عدم وجود كلمات مرور افتراضية قيد الاستخدام لإطار عمل التطبيق أو أي مكونات مستخدمة من قبل التطبيق (مثل "admin/password").
١-٨	التحقق من وجود ضابط مصادر (Resource Governor) لتوفير الحماية من الهجوم التخميني العمودي (Vertical Brute Forcing) (وهو هجوم يحاول اختراق حساب واحد باستخدام كافة كلمات المرور المحتملة) والهجوم التخميني الأفقي (Horizontal Brute Forcing) (وهو هجوم يحاول اختراق جميع الحسابات باستخدام كلمة مرور واحدة مثل "Password1"). ويجب ألا يكون هناك تأخير في إدخال بيانات الاعتماد الصحيحة. فعلى سبيل المثال، يجب ضبط إعدادات عنوان بروتوكول الإنترنت لمصدر الهجوم التخميني بحيث يتم إغلاقه بعد

١	عمليات التحقق من الهوية (OWASP:A2:2017 - إجراءات التحقق من الهوية غير الآمنة) Authentication (OWASP:A2:2017 – Broken Authentication)
	٦٠ دقيقة، ويتم إغلاق الحساب بعد ١٥ دقيقة. ويجب أن تكون آليتا الضبط فاعلتين بشكل متزامن للحماية من الهجمات التشخيصية والموزعة.
١-٩	التحقق من أن كافة ضوابط التحقق من الهوية فعالة من جهة الخادم.
١-١٠	التحقق من أن حقول كلمات المرور تسمح باستخدام عبارات مرور، ولا تمنع استخدام عبارات مرور طويلة أو معقدة للغاية، وتوفر حماية كافية من استخدام كلمات المرور الدراجة.
١-١١	التحقق من أن كافة وظائف إدارة الحسابات، (مثل التسجيل، أو تحديث الملف التعريفي، أو "نسيت اسم المستخدم"، أو "نسيت كلمة المرور"، أو رمز التعريف غير المفعل/المفقود، أو مكتب المساعدة، أو الاستجابة الصوتية التفاعلية "IVR")، والتي يمكن أن تستعيد صلاحية الوصول إلى الحساب، قادرة على مقاومة الهجمات بنفس مستوى الآلية الأساسية للتحقق من الهوية.
١-١٢	التحقق من أن المستخدمين يمكنهم تغيير بيانات اعتمادهم باستخدام آلية مقاومة للهجمات تتمتع بنفس قدرة الآلية الأساسية للتحقق من الهوية على مقاومة الهجمات. عند تغيير كلمات المرور، يجب إدخال كلمة المرور الحالية قبل إدخال كلمة المرور الجديدة وأن يتبع ذلك عملية إعادة تحقق من المستخدم.
١-١٣	التحقق من انتهاء صلاحية بيانات الاعتماد بعد مرور فترة زمنية يتم إعدادها إدارياً. ويجب أن تكون فترة انتهاء صلاحية كلمة المرور قصيرة بناءً على حساسية التطبيق، مما يفرض بالتالي تغيير كلمة المرور بشكل أسرع.
١-١٤	التحقق من تسجيل كافة قرارات التحقق من الهوية بما في ذلك "المباعدات الخطية" و"الأقفال المؤقتة".
١-١٥	التحقق من أن كلمات مرور الحسابات مجزئة عشوائياً باستخدام طريقة تجزئة عشوائية خاصة لكل حساب (مثل هوية مستخدم الإنترنت أو إنشاء الحساب) واختزالها قبل التخزين.
١-١٦	التحقق من أن كافة بيانات اعتماد التحقق من الهوية للوصول للخدمات الخارجية بالنسبة للتطبيق مشفرة ومخزنة في موقع محمي (وليس في شفرة مصدرية).
١-١٧	التحقق من أن نسيان كلمة المرور ومسارات الاستعادة ترسل رمز تفعيل أو تحقّق من الهوية متعدّد العناصر له وقت محدد (مثل الرسائل النصية، أو رموز تعريفية، أو تطبيقات الهواتف المحمولة، أو غيرها) بدلاً من إرسال كلمة المرور.
١-١٨	التحقق من أن وظيفة "نسيت كلمة المرور" لا تغلق الحساب أو تلغي تفعيله إلا بعد أن ينجح المستخدم في تغيير كلمة المرور.
١-١٩	التحقق من عدم وجود أسئلة وإجابات معرفية مشتركة (ما يسمى بالأسئلة والإجابات "السرية").
١-٢٠	التحقق من إمكانية إعداد النظام وضبطه بحيث لا يسمح باستخدام أرقام قابلة للإعداد من كلمات مرور سابقة.
١-٢١	التحقق من تنفيذ كافة ضوابط التحقق من الهوية مركزياً (بما في ذلك المكتبات التي تستدعي خدمات تحقق خارجية).
١-٢٢	التحقق من طلب إعادة التحقق من الهوية أو تحقق الإعداد أو التحقق من الهوية المتغير، أو الرسالة النصية أو التطبيق ثنائي العوامل أو توقيع المعاملة قبل السماح بأي عمليات حساسة على التطبيق وفقاً للملف التعريفي للمخاطر الخاصة بالتطبيق.
١-٢٣	التحقق من وجود وظيفة لإلغاء تفعيل بيانات اعتماد المستخدم أو إبطالها في حال وقوع انتهاك أمني.
١-٢٤	التحقق من تشفير كلمة المرور وفقاً للمعايير والإجراءات ذات العلاقة.
١-٢٥	إذا كان التطبيق يدير مخزن بيانات اعتماد، فإنه يجب أن يضمن تخزين قيمة الاختزال باتجاه واحد وبطريقة مشفرة بدرجة تعقيد عالية لكلمات المرور، وأن الجدول والملف الذي يخزن كلمات المرور والمفاتيح يمكن الكتابة عليه فقط عن طريق التطبيق. (يجب عدم استخدام خوارزمية "MD5" قدر الإمكان).
١-٢٦	فصل منطق التحقق من الهوية عن المصدر الذي يتم طلبه، واستخدام إعادة التوجيه من وإلى مراقبة التحقق من الهوية المركزي.

١	عمليات التحقق من الهوية (OWASP:A2:2017 - إجراءات التحقق من الهوية غير الآمنة) Authentication (OWASP:A2:2017 – Broken Authentication)
١-٢٧	يجب ألا تشير رسائل فشل التحقق من الهوية إلى الجزء غير الصحيح من بيانات التحقق من الهوية. فعلى سبيل المثال، بدلاً من استخدام "اسم مستخدم غير صحيح" أو "كلمة مرور غير صحيحة"، يجب استخدام "اسم مستخدم غير صحيح أو كلمة مرور غير صحيحة" لكلا الحالتين. ويجب أن تكون رسائل الأخطاء متطابقة في الشفرة المصدرية وعند عرضها.
١-٢٨	يجب تطبيق متطلبات درجة تعقيد كلمة المرور الواردة في السياسة أو اللائحة، كما يجب أن تكون بيانات اعتماد التحقق من الهوية كافية لمواجهة الهجمات التي تعتبر شائعة بالنسبة للتهديدات الموجودة في بيئة التثبيت. ويجب التحقق من أن كلمة المرور تتضمن كحد أدنى ما يلي: • حرف كبير واحد على الأقل (A-Z). • حرف صغير واحد على الأقل (a-z). • رقم واحد على الأقل (٠-٩). • رمز خاص واحد على الأقل مثل:(!"#$%&'()*+،-./:;<=>؟@[\]^_`{|}~"). كما يجب التحقق من أن كلمة المرور لا تتضمن على الأقل ما يلي: • أكثر من رقمين أو رمزين متطابقين متتاليين (مثل "١١١" و"aa"). • أرقام أو رموز متسلسلة (مثل "١٢٣"، أو "٧٨٩"، أو"abc"). • نفس اسم المستخدم. • كلمات قاموسية ("password"، أو "p@ssw0rd"، أو "secret123").
١-٢٩	إنفاذ إلغاء تفعيل الحساب بعد عدد محدد من محاولات تسجيل الدخول غير الصحيحة (على سبيل المثال، خمس محاولات للتطبيقات غير الهامة وثلاث محاولات للتطبيقات الحساسة). ويجب إلغاء تفعيل الحساب لفترة زمنية معينة تكون كافية لإحباط محاولات الهجوم التخميني لبيانات الاعتماد شريطة ألا تكون هذه المدة طويلة بحيث تسمح بتنفيذ هجمات حجب الخدمة (مثلاً إلغاء التفعيل لمدة ٣٠ دقيقة فقط).
١-٣٠	يجب إبلاغ المستخدم بآخر استخدام للحساب (سواءً كان ناجحاً أم لا) عند تسجيله الدخول بنجاح.

يعرض الجدول التالي: (جدول رقم: ١٦ - إجراءات التحقق من الهوية غير الآمنة) إجراءات إدارة الجلسات.

٢	إدارة الجلسات (OWASP:A2: 2017 - إجراءات التحقق من الهوية غير الآمنة) Session Management (OWASP:A2:2017 – Broken Authentication)
٢-١	التحقق من استخدام التطبيق لتنفيذ التحكم بإدارة الجلسة التلقائية الخاصة بإطار العمل.
٢-٢	التحقق من إبطال الجلسات عند تسجيل خروج المستخدم.
٢-٣	التحقق من انتهاء وقت الجلسات بعد مرور فترة معينة من عدم النشاط.
٢-٤	التحقق من أن كافة الصفحات التي تقتضي التحقق من الهوية للوصول إليها تتضمن روابط لتسجيل الخروج.
٢-٥	التحقق من أن هوية الجلسة غير مكشوفة أبداً إلا في عناوين ملفات الارتباط (Cookie، وتحديداً في شريط العنوان (URL) أو رسائل الخطأ أو السجلات. ويتضمن هذا التحقق من أن التطبيق لا يدعم قيام شريط العنوان (URL) بإعادة كتابة جلسات الملفات التعريفية.
٢-٦	التحقق من تغيير هوية الجلسة أو مسحها عند تسجيل الخروج.

٢	إدارة الجلسات (OWASP:A2: 2017 - إجراءات التحقق من الهوية غير الآمنة) Session Management (OWASP:A2:2017 – Broken Authentication)
٢-٧	التحقق من أن الرموز التعريفية للجلسات المصادق عليها باستخدام ملفات الارتباط محمية باستخدام آلية "HttpOnly" (عدم عرض ملفات الارتباط عند المستخدم).
٢-٨	التحقق من أن الرموز التعريفية للجلسات المصادق عليها باستخدام ملفات الارتباط محمية بخاصية "Secure" وأن عناوين أمن النقل المقيد موجودة (مثل: "Strict-Transport-Security: max-age=60000; includeSubDomains").
٢-٩	التحقق من تغيير هوية الجلسة عند تسجيل الدخول لمنع سرقة بيانات الجلسة.
٢-١٠	التحقق من تغيير هوية الجلسة عند إعادة التحقق من الهوية.
٢-١١	التحقق من أن التطبيق يتعرف على هويات الجلسات الصادرة عن طريق إطار عمل التطبيق نفسه ويعتبر هذه الهويات فقط صحيحة.
٢-١٢	التحقق من أن الرموز التعريفية للجلسات المصادق عليها طويلة وعشوائية بالقدر الكافي لمواجهة الهجمات التي تعتبر تهديدات شائعة في بيئة التثبيت.
٢-١٣	التحقق من أن الرموز التعريفية للجلسات المصادق عليها والتي تستخدم ملفات الارتباط لها مسار محدد بقيمة حصرية ملائمة لذلك الموقع. ويجب عدم تحديد تقييد خاصية ملف ارتباط النطاق إلا إذا كانت الأعمال تقتضي ذلك، كعملية تسجيل دخول موحد.
٢-١٤	التحقق من أن التطبيق لا يسمح بجلسات مستخدم متزامنة مكررة صادرة من أجهزة مختلفة.
٢-١٥	التحقق من انتهاء وقت الجلسات بعد مرور الحد الأقصى لفترة زمنية تم إعدادها إدارياً بغض النظر عن النشاط (أي وقت انتهاء مطلق).
٢-١٦	إصدار هوية جديدة للجلسة في حال تغيير أمن الاتصال من بروتوكول نقل النص التشعبي (HTTP) إلى بروتوكول نقل النص التشعبي الآمن (HTTPS)، والذي قد يحدث خلال عملية التحقق من الهوية. من المستحسن استخدام بروتوكول نقل النص التشعبي الآمن (HTTPS) باستمرار في التطبيق بدلاً من التنقل بين بروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل النص التشعبي الآمن (HTTPS).

بالإضافة لما سبق، يشتمل الجدول التالي: (جدول رقم: ١٧ - إجراءات التحكم بالوصول غير الآمنة) على العمليات والإجراءات الواجب اتخاذها للتحكم بالوصول غير الآمن لشبكة الجامعة.

٣	التحكم بالوصول (OWASP:A5:2017 - إجراءات التحكم بالوصول غير الآمنة) Access Control (OWASP:A5:2017 – Broken Access Control)
٣-١	يجب عمل مراجعة دورة لصلاحيات المستخدمين وتحديث هذه الصلاحيات والتحقق من أن المستخدمين يمكنهم الوصول فقط إلى الوظائف أو الخدمات الآمنة التي يملكون تصاريح وصلاحيات خاصة لها.
٣-٢	التحقق من أن المستخدمين يمكنهم الوصول فقط إلى العناوين الآمنة Secured URLs)) التي يملكون تصاريح وصلاحيات خاصة لها.
٣-٣	التحقق من أن المستخدمين يمكنهم الوصول فقط إلى ملفات البيانات الآمنة التي يملكون تصاريح وصلاحيات خاصة لها.
٣-٤	التحقق من أن مرجعيات الكائنات المباشرة محمية بحيث يمكن الوصول فقط إلى الكائنات المصرح بها لكل مستخدم.
٣-٥	التحقق من إلغاء تفعيل تصفح الدليل (Directory Browsing) إلا إذا كان ذلك مطلوباً.
٣-٦	التحقق من أن المستخدم يمكنه الوصول فقط إلى المعلومات المحمية التي يملك تصاريح وصلاحيات خاصة لها (على سبيل المثال، من خلال تطبيق ضوابط لحماية مرجعيات الكائنات من التلاعب المباشر والوصول غير المصرح به إلى البيانات).
٣-٧	التحقق من إخفاق ضوابط الوصول بصورة آمنة.
٣-٨	التحقق من أن نفس قواعد التحكم بالوصول المتضمنة في طبقة العرض مطبقة على الخادم بحسب دور المستخدم، بحيث لا يمكن إعادة تفعيل الضوابط والمعايير أو إعادة إضافتها من مستخدمين يمتلكون مزايا وصلاحيات أعلى.

٣	التحكم بالوصول (OWASP:A5:2017 - إجراءات التحكم بالوصول غير الآمنة) Access Control (OWASP:A5:2017 – Broken Access Control)
٣-٩	التحقق من أن كافة خصائص المستخدمين والبيانات ومعلومات السياسة المستخدمة من قبل ضوابط الوصول لا يمكن التلاعب بها من قبل المستخدمين إلا إذا كان مصرحاً لهم بذلك تحديداً.
٣-١٠	التحقق من أن كافة ضوابط الوصول فعالة من جهة الخادم.
٣-١١	التحقق من أن قرارات التحكم بالوصول يمكن تسجيلها وأن كافة القرارات غير الناجحة قد تم تسجيلها.
٣-١٢	التحقق من أن التطبيق أو إطار العمل يصدر رموزاً تعريفية عشوائية معقدة مضادة لتزوير الطلب عبر المواقع Cross-Site Request Forgery "CSRF")، وتكون هذه الرموز خاصة بالمستخدم باعتبارها جزءاً من كافة المعاملات عالية القيمة أو الوصول إلى المعلومات المحمية، وأن التطبيق يتحقق من وجود هذه الرموز التعريفية بالقيمة الملائمة للمستخدم الحالي عند معالجة هذه الطلبات.
٣-١٣	الحماية التراكمية للتحكم بالوصول- التحقق من أن النظام يستطيع توفير الحماية من الوصول التراكمي، أو المستمر للوظائف المحمية، أو المصادر، أو البيانات، وذلك من خلال استخدام ضابط مصادر (Resource Governor) على سبيل المثال، للحد من عدد حالات التسجيل لكل ساعة أو منع مستخدم فردي من سحب بيانات قاعدة البيانات بأكملها.
٣-١٤	التحقق من وجود آلية مركزية (بما في ذلك المكتبات التي تستدعي خدمات تصاريح وصلاحيات خارجية) للتحكم بالوصول إلى كل نوع من المصادر المحمية.
٣-١٥	التحقق من الفصل بين المنطق الذي يتمتع بمزايا وصلاحيات عن شفرات التطبيق الأخرى.
٣-١٦	تطبيق ضوابط الوصول الملائمة إلى المعلومات المحمية المخزنة على الخادم. وتشمل هذه المعلومات البيانات المخزنة والملفات المؤقتة والبيانات التي يمكن الوصول إليها فقط من قبل مستخدمين نظام محددين.
٣-١٧	التحقق من أن حسابات الخدمة أو الحسابات التي تدعم الاتصالات من الأنظمة الخارجية أو إليها تمتلك الحد الأدنى من الصلاحيات والامتيازات.
٣-١٨	التحقق من تطبيق تدقيق الحسابات وإلغاء تفعيل الحسابات غير المستخدمة (على سبيل المثال، بعد مرور أكثر من ٣٠ يوماً من تاريخ انتهاء صلاحية كلمة مرور الحساب).
٣-١٩	في حال السماح بالجلسات الطويلة المصادق عليها، يجب إعادة التحقق دورياً من تصاريح وصلاحيات المستخدم لضمان عدم تغير مزاياه، وفي حال تغيرها، يجب تسجيل خروج المستخدم وفرض عملية إعادة التحقق من الهوية.
٣-٢٠	التحقق من أن التطبيق يدعم إلغاء تفعيل الحسابات وإنهاء الجلسات عند توقف التصاريح والصلاحيات (على سبيل المثال، عند حدوث تغيير في الدور، أو في حالة التوظيف، أو إجراءات الأعمال، أو غيرها).

كما يتبين من الجدول التالي: (جدول رقم: ١٧ - اعتماد المدخلات) على عمليات التحقق من إجراءات الحقن والإدخال للبرمجة النصية عبر المواقع.

٤	اعتماد المدخلات (OWASP:A1:2017 - الحقن والإدخال و OWASP:A7:2017 - البرمجة النصية عبر المو اقع) Input validation (OWASP:A1:2017 – Injection & OWASP:A7:2017 – Cross-Site Scripting)
٤-١	التحقق من أن بيئة التشغيل غير معرضة لتجاوز سعة المخزن المؤقت، وأن ضوابط الأمن تمنع تجاوز سعة المخزن المؤقت.
٤-٢	التحقق من أن بيئة التشغيل غير معرضة لحقن تعليمات الاستعلام البنيوية Injection(SQL)، وأن ضوابط الأمن تمنع حقن تعليمات الاستعلام البنيوية Injection (SQL).
٤-٣	التحقق من أن بيئة التشغيل غير معرضة لحقن النصوص البرمجية عبر المواقع (XSS)، وأن ضوابط الأمن تمنع حقن النصوص البرمجية عبر المواقع (XSS).

٤	اعتماد المدخلات (OWASP:A1:2017 - الحقن والإدخال و OWASP:A7:2017 - البرمجة النصية عبر المو اقع) Input validation (OWASP:A1:2017 – Injection & OWASP:A7:2017 – Cross-Site Scripting)
٤-٤	التحقق من أن بيئة التشغيل غير معرضة لحقن بروتوكول النفاذ إلى الدليل البسيط (LDAP Injection) وأن ضوابط الأمن تمنع حقن بروتوكول النفاذ إلى الدليل البسيط (LDAP Injection).
٤-٥	التحقق من أن بيئة التشغيل غير معرضة لحقن أوامر نظام التشغيل OS (Command Injection)، وأن ضوابط الأمن تمنع حقن أوامر نظام التشغيل OS (Command Injection).
٤-٦	التحقق من نوع البيانات ونطاقها وطولها (إذا أمكن).
٤-٧	عند الحاجة إلى السماح برموز خطرة محتملة كمدخلات، يجب التأكد من تطبيق ضوابط إضافية مثل ترميز المدخلات، وحماية واجهات برمجة التطبيقات الخاصة بالمهام، ومعرفة الجهات التي تستخدم تلك البيانات طوال فترة استخدام التطبيق. وتشمل الأمثلة على الرموز الخطرة الشائعة الآتي: (< > " ' % ( ) & + \ \ '\ "\").
٤-٨	التأكد من أن جميع عمليات التحقق من صحة المدخلات تتم بواسطة روتين مركزي للتحقق من صحة المدخلات للتطبيق.
٤-٩	التحقق من أن كافة عمليات التحقق الفاشلة تؤدي إلى رفض المدخلات أو تدقيقها.
٤-١٠	التحقق من تنفيذ كافة إجراءات التحقق أو إجراءات تطوير التطبيقات وإنفاذها على الخادم.
٤-١١	التحقق من التخلص من كافة البيانات غير الموثوقة والتي تعتبر مخرجات بالنسبة للغة "HTML" (بما في ذلك عناصر لغة "HTML" وخصائصها، وقيم بيانات لغة "JavaScript"، وكتل الصفحات النمطية المتسلسلة "CSS Blocks"، وخصائص شريط العنوان "URL") بصورة ملائمة لمحتوى التطبيق.
٤-١٢	التحقق من أن مجموعات الرموز، مثل "UTF-8"، محددة لكافة مصادر المدخلات.
٤-١٣	التحقق من أن كافة البيانات المدخلة موحدة لكافة برمجيات فك تشفير أو برمجيات تفسير البيانات المرسلة إلى العميل قبل مصادقتها.
٤-١٤	إذا كان إطار عمل التطبيق يسمح بالتخصيص التلقائي الضخم للمعايير (ويسمى أيضاً ربط المتغيرات التلقائي) من طلب وارد إلى نموذج، فيجب التحقق من أن الحقول الحساسة أمنياً مثل "رصيد الحساب" أو "الدور" أو "كلمة المرور" محمية من الربط التلقائي الخبيث.
٤-١٥	التحقق من أن التطبيق محمي من هجمات تلوث متغيرات بروتوكول نقل النص التشعبي (HTTP)، خصوصاً إذا كان إطار عمل التطبيق لا يميز بين مصادر متغيرات الطلب (مثل طلب "GET"، وطلب "POST"، وملفات الارتباط، والعناوين، والبيئة، وغيرها).
٤-١٦	التحقق من أن التطبيق يستخدم ضابط تحقق من المدخلات واحد لكل نوع من البيانات التي يتم قبولها.
٤-١٧	التحقق من تسجيل كافة حالات الإخفاق في التحقق من المدخلات.
٤-١٨	التحقق من أن كل نوع من عمليات ترميز المخرجات أو التخلص منها التي يقوم بها التطبيق له ضابط أمني واحد للوجهة المقصودة.

ويظهر في الجدول التالي: (جدول رقم: ١٨ - إلغاء التسلسل غير الآمن) إجراءات وقيود التسلسل غير الآمن.

٥	إلغاء التسلسل غير الآمن (OWASP:A8:2017- إلغاء التسلسل غير الآمن) Insecure Deserialization (OWASP:A8:2017 – Insecure Deserialization)
٥-١	تطبيق عمليات التحقق من سلامة المعلومات، مثل التواقيع الرقمية، لأي كائنات متسلسلة لمنع إنشاء كائنات عدائية أو التلاعب بالبيانات.
٥-٢	إنفاذ قيود محددة خلال إلغاء التسلسل قبل إنشاء الكائن لأن الشفرة تتوقع عادة مجموعة فئات قابلة للتحديد. من غير المستحسن الاعتماد على هذا الأسلوب فقط نظراً إلى وجود طرق لتجاوزه.
٥-٣	عزل الشفرة التي يتم إلغاء تسلسلها وتشغيلها في بيئات متدنية المزايا والصلاحيات حيثما أمكن.
٥-٤	تسجيل استثناءات إلغاء التسلسل وحالات الإخفاق، مثل الحالات التي لا يكون فيها النوع الوارد هو النوع المتوقع أو التي يحدد فيها إلغاء تسلسل الاستثناءات.

٥	إلغاء التسلسل غير الآمن (OWASP:A8:2017- إلغاء التسلسل غير الآمن) Insecure Deserialization (OWASP:A8:2017 – Insecure Deserialization)
	تقييد أو مراقبة الربط البيني الوارد والصادر في الشبكة من الحاويات أو الخوادم التي تم إلغاء تسلسلها.
	مراقبة إلغاء التسلسل والتنبيه إذا كان المستخدم يلغي التسلسل باستمرار.

ويستعرض الجدول التالي: (جدول رقم: ١٩ - التشفير) إجراءات التشفير الواجب اتخاذها في حال تعرّض المعلومات المحمية للمخاطر.

٦	التشفير (OWASP:A3:2017 - تعرّض المعلومات المحمية للمخاطر) Cryptography (OWASP:A3:2017 – Protected Data Exposure)
١-٦	التحقق من أن كافة دالات التشفير المستخدمة لحماية الأسرار من مستخدم التطبيق مطبقة على الخادم.
٢-٦	التحقق من أن كافة وحدات التشفير تخفق بصورة آمنة.
٣-٦	التحقق من حماية أي أسرار رئيسية من الوصول غير المصرح به (السر الرئيسي هو بيانات اعتماد التطبيق المخزنة كنص غير مشفر على القرص والتي تستخدم لحماية الوصول إلى معلومات الإعدادات الأمنية).
٤-٦	التحقق من أن كافة الأرقام العشوائية، وأسماء الملفات العشوائية، والمعرفات الموحدة (GUIDs)، وسلاسل الحروف العشوائية (Strings) صادرة من مولد الأرقام العشوائية المعتمد لنموذج التشفير، وذلك عندما يكون الهدف من هذه القيم العشوائية هو جعل الجهة المهاجمة غير قادرة على تخمينها.
٥-٦	التحقق من أن نماذج التشفير المستخدمة في التطبيق قد تم التحقق منها وفقاً للسياسات والإجراءات ذات العلاقة.
٦-٦	التحقق من أن نماذج التشفير تعمل بنظامها المعتمد وفقاً للسياسات والإجراءات ذات العلاقة.
٧-٦	التحقق من وجود سياسة صريحة حول كيفية إدارة مفاتيح التشفير (مثل كيفية إصدارها وتوزيعها وإلغائها وانتهاء صلاحيتها) والتحقق من تطبيق هذه السياسة بصورة ملائمة.
٨-٦	التحقق من وجود عدم الإنكار(Non-Repudiation) من خلال التشفير (التوقيع الرقمي) للمعاملات المالية والتجارة الإلكترونية والسجلات.
٩-٦	التحقق من حماية كافة مفاتيح التشفير بصورة ملائمة. في حال تعرض المفتاح لانتهاك أمني، فإنه لا يمكن الوثوق به ويجب استبداله أو إلغاؤه.
١٠-٦	التحقق من تشفير المعلومات القابلة لتحديد الهوية (PII) والمعلومات المحمية والبيانات المخزنة عندما لا تكون قيد الاستخدام.

كما يظهر في الجدول التالي: (جدول رقم: ٢٠ - التعامل مع الأخطاء وتسجيلها) إجراءات التعامل مع عدم كفاية وفاعلية التسجيل والمراقبة.

٧	التعامل مع الأخطاء وتسجيلها (OWASP:A10:2017 - عدم كفاية وفاعلية التسجيل والمراقبة) Error Handling and Logging (OWASP:A10:2017 – Insufficient Logging & Monitoring)
١-٧	ضمان إجراء التحقق الصريح من الأخطاء للبرمجيات المطورة داخلياً، وتوثيقه لكافة المدخلات، بما في ذلك الحجم ونوع البيانات والنطاقات أو الصيغ المسموحة.
٢-٧	التحقق من أن التطبيق لا يظهر رسائل خطأ أو يكدس آثاراً تتضمن معلومات محمية، بما في ذلك هوية الجلسة والمعلومات الشخصية، والتي يمكن أن تساعد الجهة المهاجمة على تنفيذ أنشطتها.
٣-٧	التحقق من تنفيذ جميع عمليات التعامل مع الأخطاء على أجهزة موثوقة.

٧	التعامل مع الأخطاء وتسجيلها (OWASP:A10:2017 - عدم كفاية وفاعلية التسجيل والمراقبة) Error Handling and Logging (OWASP:A10:2017 – Insufficient Logging & Monitoring)
٧-٤	التحقق من تطبيق كافة ضوابط التسجيل على الخادم.
٧-٥	التحقق من أن منطق التعامل مع الأخطاء في الضوابط الأمنية يحجب الوصول تلقائياً.
٧-٦	التحقق من أن ضوابط التسجيل الأمنية تسمح بتسجيل أحداث النجاح والإخفاق التي تم تحديدها باعتبارها مهمة أمنياً.
٧-٧	التحقق من أن كل حدث في السجل يتضمن ختماً زمنياً من مصدر موثوق، ومستوى شدة الحدث، ومؤشراً على أن الحدث مهم أمنياً (إذا كان مختلطاً مع سجلات أخرى)، وهوية المستخدم الذي تسبب بالحدث (إذا كان هناك مستخدم مرتبط بالحدث)، ومصدر عنوان بروتوكول الإنترنت للطلب المصاحب للحدث سواءً كان الحدث ناجحاً أو فاشلاً، ووصفاً للحدث.
٧-٨	التحقق من أن كافة السجلات محمية من الوصول غير المصرح به والتعديل.
٧-٩	التحقق من أن التطبيق لا يسجل معلومات محمية خاصة بالتطبيق، بما في ذلك هوية الجلسة والمعلومات الشخصية أو المحمية، والتي يمكن أن تساعد الجهة المهاجمة على تنفيذ أنشطتها.
٧-١٠	التحقق من توفر أداة تحليل السجل مما يسمح للمحلل بالبحث عن أحداث السجل بناءً على تركيبة من معايير البحث في كافة الحقول في صيغة السجل المدعومة من النظام.
٧-١١	التحقق من عدم تنفيذ كافة الأحداث التي تتضمن بيانات غير موثوقة باعتبارها شفرة في برمجيات استعراض السجلات المعنية.
٧-١٢	التحقق من وجود تنفيذ تسجيل موحد مستخدم في التطبيق.
٧-١٣	التحقق من أن السجلات لها إجراء منتظم موحد للنسخ الاحتياطية أو الأرشفة.
٧-١٤	تطبيق "التعامل مع الاستثناءات في الشفرات" حيثما أمكن.
٧-١٥	التحقق من أن السجلات أدناه مفعلة: • سجل يشمل كل حالات الإخفاق في التحقق من المدخلات. • سجل يشمل كل محاولات التحقق من الهوية، وخصوصاً حالات الإخفاق. • سجل يشمل كل حالات الإخفاق في التحكم بالوصول. • سجل يشمل كل أحداث التلاعب الظاهرة، بما في ذلك التغييرات غير المتوقعة على حالة البيانات. • سجل يشمل كل محاولات الاتصال بالرموز التعريفية لجلسة منتهية الصلاحية أو غير صحيحة. • سجل يشمل كل استثناءات النظام. • سجل يشمل كل الوظائف الإدارية، بما في ذلك التغييرات على إعدادات الضبط والتهيئة الأمنية. • سجل يشمل كل حالات إخفاق اتصال أمن طبقة النقل بأجهزة النقطة النهائية. • سجل يشمل كل حالات إخفاق نموذج التشفير.

كما يتضح من خلال الجدول التالي: (جدول رقم: ٢١ - حماية المعلومات) إجراءات الواجب تطبيقها في حال تعرّض المعلومات المحمية للمخاطر.

٨	حماية المعلومات (OWASP:A3:2017 - تعرّض المعلومات المحمية للمخاطر) Data Protection (OWASP:A3:2017 – Protected Data Exposure)
٨-١	التحقق من إلغاء تفعيل تخزين النماذج التي تتضمن معلومات محمية لدى العميل، بما في ذلك خصائص الإكمال التلقائي.
٨-٢	التحقق من إرسال كافة المعلومات المحمية إلى الخادم في متن رسالة بروتوكول نقل النص التشعبي (HTTP)، (أي منع استخدام معايير شريط العنوان "URL" لإرسال البيانات المحمية).

٨	حماية المعلومات (OWASP:A3:2017 - تعرّض المعلومات المحمية للمخاطر) Data Protection (OWASP:A3:2017 – Protected Data Exposure)
٨-٣	التحقق من أن كافة النسخ المخزنة أو المؤقتة للمعلومات المحمية المخزنة على الخادم محمية من الوصول غير المصرح به، والتأكد من حذف الملفات العاملة المؤقتة بمجرد انقضاء الحاجة لها.
٨-٤	إلغاء تفعيل التخزين أو حفظ النسخ المؤقتة للصفحات التي تتضمن معلومات محمية لدى العميل، والتحقق من أن هذه النسخ محمية من الوصول غير المصرح به أو مسحها أو إلغاء صلاحيتها بعد وصول المستخدم المصرح له إليها. (يمكن استخدام "Cache-Control: no-store" مع ضابط عنوان بروتوكول نقل النص التشعبي "HTTP". "Pragma: no-cache"، وهو أقل فاعلية، ولكنه متوافق مع النسخ الأقدم "1.0" من بروتوكول نقل النص التشعبي "HTTP").
٨-٥	التحقق من تحديد قائمة بالمعلومات المحمية التي يعالجها التطبيق، والتأكد من وجود سياسة صريحة حول كيفية التحكم بالوصول إلى هذه المعلومات، ومتى يجب تشفيرها (أثناء عدم الاستخدام وأثناء النقل والاستخدام)، والتحقق من تطبيق هذه السياسة بصورة ملائمة.
٨-٦	التحقق من وجود طريقة لحذف كل أنواع المعلومات المحمية الموجودة في التطبيق عند نهاية فترة الاحتفاظ المطلوبة.
٨-٧	التحقق من أن التطبيق يقلل عدد المعايير المرسلة إلى الأنظمة غير الموثوقة مثل الحقول المخفية ومتغيرات "Ajax" وملفات الارتباط وقيم العناوين.
٨-٨	التحقق من قدرة التطبيق على كشف الأرقام غير الطبيعية لطلبات المعلومات والتنبيه بشأنها، أو معالجة المعاملات عالية القيمة لدور المستخدم مثل سحب الشاشة، أو الاستخدام التلقائي لاستخلاص خدمات الويب، أو منع فقدان البيانات. على سبيل المثال، يجب ألا يكون المستخدم العادي قادراً على الوصول إلى أكثر من ٥ سجلات في الساعة أو أكثر من ٣٠ سجلاً في اليوم.
٨-٩	التحقق من أن بيانات الاعتماد التي يستخدمها التطبيق على الخادم، مثل اتصال قاعدة البيانات، وكلمة المرور، والمفاتيح السرية للتشفير، ليست مثبتة في الشفرة. ويجب تخزين أي بيانات اعتماد في ملف إعدادات منفصل على نظام موثوق وتشفيرها.
٨-١٠	التحقق من أن خصائص الإكمال التلقائي غير مفعلة على النماذج باستثناء النماذج التي تتضمن معلومات محمية، بما في ذلك التحقق من الهوية.

يستعرض الجدول التالي: (جدول رقم: ٢٢ - أمن الاتصالات) إجراءات الإعدادات الأمنية الخاطئة.

٩	أمن الاتصالات (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة) Communication Security (OWASP:A6:2017 – Security Misconfiguration)
٩-١	التحقق من أنه يمكن بناء مسار من جهة إصدار شهادات موثوقة لكل شهادة تشفير خادم أمن طبقة النقل (TLS)، وأنه قد تم التحقق من صلاحية شهادة كل خادم.
٩-٢	التحقق من استخدام أحدث إصدار من أمن طبقة النقل (TLS) في كافة الاتصالات (بما في ذلك الاتصالات الخارجية واتصالات أجهزة النقطة النهائية) التي تم مصادقتها أو التي تتضمن معلومات أو وظائف محمية.
٩-٣	التحقق من تسجيل حالات إخفاق اتصالات أمن طبقة النقل (TLS) بأجهزة النقطة النهائية.
٩-٤	التحقق من المصادقة على كافة الاتصالات مع الأنظمة الخارجية التي تتضمن معلومات أو وظائف محمية.
٩-٥	التحقق من أن كافة الاتصالات مع الأنظمة الخارجية التي تتضمن معلومات أو وظائف محمية تستخدم حساباً تم إعداده ومنحه الحد الأدنى من المزايا والصلاحيات اللازمة ليعمل التطبيق بالشكل الصحيح.
٩-٦	التحقق من أن اتصالات أمن طبقة النقل (TLS) الفاشلة لا ينتج عنها اتصال غير آمن (غير مشفر).
٩-٧	التحقق من أن مسارات شهادات التشفير قد تم بناؤها والتحقق منها لكافة شهادات التشفير الخاصة بالعميل باستخدام جهات الصلاحيات الموثوقة ومعلومات الإلغاء.
٩-٨	التحقق من وجود تنفيذ أمن طبقة النقل (TLS) موحد يتم استخدامه في التطبيق وتم إعداده ليعمل في نظام عمل معتمد.

٩	أمن الاتصالات (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة) Communication Security (OWASP:A6:2017 – Security Misconfiguration)
٩-٩	التحقق من أن ترميز الرموز المحددة معرف لكافة الاتصالات (مثل "UTF-8").

وبمراجعة الجدول التالي: (جدول رقم: ٢٣ - أمن البروتوكول) فإنه يستعرض الإعدادات الأمنية الخاطئة ولغة الترميز القابلة للامتداد لجهات خارجية.

١٠	أمن البروتوكول (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة و OWASP:A4:2017 لغة الترميز القابلة للامتداد لجهات خارجية) Protocol Security (OWASP:A6:2017 – Security Misconfiguration & OWASP:A4:2017 XML External Entities)
١٠-١	التحقق من أن التطبيق يقبل مجموعة محددة فقط من طرق طلب بروتوكول نقل النص التشعبي (HTTP) مثل طلب "GET" وطلب "POST" وأن الطرق غير المستخدمة محظورة.
١٠-٢	التحقق من أن كل استجابة لبروتوكول نقل النص التشعبي (HTTP) تتضمن عنوان نوع محتوى يحدد مجموعة رموز آمنة (مثل "UTF-8").
١٠-٣	التحقق من أن عناوين بروتوكول نقل النص التشعبي (HTTP) و/أو الآليات الأخرى للمتصفحات الأقدم متضمنة من أجل الحماية من هجمات الخطف بالنقر (Click Jacking).
١٠-٤	التحقق من أن عناوين بروتوكول نقل النص التشعبي (HTTP) في الطلبات والاستجابات تتضمن فقط رموز المدونة الموحدة الأمريكية لتبادل المعلومات القابلة للطباعة (ASCII).
١٠-٥	التحقق من استخدام صيغ بيانات أقل تعقيداً مثل جافا سكريبت (JSON)، وتجنب جعل المعلومات المحمية متسلسلة.
١٠-٦	تحديث وإصلاح أو ترقية معالجات لغة الترميز القابلة للامتداد (XML) والمكتبات قيد الاستخدام في التطبيق أو نظام التشغيل الأساسي، واستخدام عمليات التحقق من الاعتماديات، وتحديث البروتوكول البسيط للوصول إلى الكائنات (SOAP) إلى إصدار ١,٢ أو إصدار أحدث.
١٠-٧	إلغاء تفعيل لغة الترميز القابلة للامتداد لجهات خارجية ومعالجة "DTD" في كافة محللات لغة الترميز القابلة للامتداد (XML) في التطبيق وفقاً لتوجيهات المشروع المفتوح لأمن تطبيقات الويب "XXE Prevention".
١٠-٨	تطبيق التحقق الإيجابي من المدخلات على الخادم (السماح بقائمة محددة) أو التصفية أو التدقيق لمنع البيانات العدائية ضمن وثائق أو عناوين أو عُقد لغة الترميز القابلة للامتداد (XML).
١٠-٩	التحقق من أن وظيفة رفع الملف بلغة الترميز القابلة للامتداد (XML) أو بلغة الأسلوب الموسع (XSL) تتحقق من لغة الترميز القابلة للامتداد (XML) باستخدام تحقق لغة كتابة الملفات المرافقة للغة (XSD) أو طريقة تحقق مشابهة.
١٠-١٠	استخدام أدوات اختبار أمن التطبيقات الثابت (SAST) واختبار أمن التطبيقات الديناميكي (DAST) للمساعدة في كشف لغة الترميز القابلة للامتداد لجهات خارجية (XXE) في الشفرة المصدرية، مع الأخذ بعين الاعتبار أن مراجعة الشفرة يدوياً هي الطريقة التي يفضل اتباعها في التطبيقات الكبيرة والمعقدة ذات العديد من التداخلات.
١٠-١١	إذا كان من غير الممكن تطبيق هذه الضوابط، يجب دراسة استخدام حزم التحديثات الافتراضية، أو البوابات الأمنية لواجهات برمجة التطبيقات، أو جدار الحماية لتطبيقات الويب لكشف هجمات لغة الترميز القابلة للامتداد لجهات خارجية (XXE) ومراقبتها وحجبها.

ويتضح من الجدول التالي: (جدول رقم: ٢٤ - الشفرة الخبيثة والثغرات) إجراءات استخدام المكونات مع الثغرات المعروفة.

١١	الشفرة الخبيثة والثغرات (OWASP:A9:2017 - استخدام المكونات مع الثغرات المعروفة) Malicious Code and Vulnerabilities (OWASP:A9:2017 – Using Components with Known Vulnerabilities)
١-١١	التحقق من عدم وجود شفرات خبيثة في أي شفرة تم تطويرها أو تعديلها بهدف إنشاء التطبيق.
٢-١١	التأكد من أن سلامة الشفرة المفسرة والمكتبات والأوامر التنفيذية وملفات الإعدادات قد تم التحقق منها باستخدام المجموعات الاختبارية أو عمليات حساب ملخص النص المميز.
٣-١١	التحقق من أن كافة الشفرات التي تطبق ضوابط التحقق من الهوية أو تستخدمها لم تتأثر بأي شفرات خبيثة.
٤-١١	التحقق من أن كافة الشفرات التي تطبق إدارة الجلسات أو تستخدمها لم تتأثر بأي شفرات خبيثة.
٥-١١	التحقق من أن كافة الشفرات التي تطبق ضوابط الوصول أو تستخدمها لم تتأثر بأي شفرات خبيثة.
٦-١١	التحقق من أن كافة ضوابط التحقق من المدخلات لم تتأثر بأي شفرات خبيثة.
٧-١١	التحقق من أن كافة الشفرات التي تطبق ضوابط التحقق من المخرجات أو تستخدمها لم تتأثر بأي شفرات خبيثة.
٨-١١	التحقق من أن كافة الشفرات التي تطبق نموذج التشفير أو تستخدمه لم تتأثر بأي شفرات خبيثة.
٩-١١	التحقق من أن كافة الشفرات التي تطبق ضوابط التعامل مع الأخطاء وتسجيلها أو تستخدمها لم تتأثر بأي شفرات خبيثة.
١٠-١١	التحقق من أن كافة الأنشطة الخبيثة قد خضعت لتقنية الحماية المعزولة (Sandboxing).
١١-١١	التحقق من التخلص من المعلومات المحمية المخزنة في الذاكرة بسرعة عند عدم الحاجة لها.
١٢-١١	تحديث المكونات بأحدث التحديثات والإصلاحات عند معرفة المستخدم بالثغرات المنشورة.
١٣-١١	إلغاء الاعتماديات غير المستخدمة والخصائص غير اللازمة والمكونات والملفات والوثائق.
١٤-١١	عمل قائمة جرد مستمرة لإصدارات المكونات من طرف العميل والخادم (مثل أطر العمل والمكتبات) واعتمادياتها باستخدام أدوات مثل الإصدارات، و"DependencyCheck"، و"retire.js"، وغيرها، والمراقبة المستمرة للمصادر مثل تعداد الثغرات الشائعة (CVE) وقاعدة بيانات الثغرات الوطنية (NVD) بحثاً عن الثغرات في المكونات، إلى جانب استخدام أدوات تحليل تكوين البرمجيات من أجل أتمتة العملية، والاشتراك في تنبيهات البريد الإلكتروني من أجل الثغرات الأمنية ذات العلاقة بالمكونات قيد الاستخدام.
١٥-١١	الحصول على المكونات من مصادر رسمية وعبر روابط محمية فقط، وتفضيل الحزم الموقعة لتقليل فرص وجود مكون خبيث معدل.
١٦-١١	مراقبة المكتبات والمكونات التي لا تتوافر لها صيانة أو ليس للإصدارات القديمة منها تحديثات وإصلاحات أمنية. إذا كان تثبيت حزم التحديثات غير ممكناً، يجب دراسة تثبيت التحديثات والإصلاحات الافتراضية لمراقبة المشكلات المكتشفة أو كشفها أو الحماية منها.

يتضح من خلال الجدول التالي: (جدول رقم: ٢٥ - قواعد العمل) عمليات التحقق من عمليات منطق وتسلسل الأعمال.

١٢	قواعد العمل (Business Logic)
١-١٢	التحقق من عمليات التطبيق ومن كافة تدفقات قواعد العمل عالية القيمة في بيئة موثوقة مثل الخادم المحمي والمراقب.
٢-١٢	التحقق من أن التطبيق لا يسمح بمعاملات عالية القيمة منتحلة، مثل السماح للمستخدم المهاجم (أ) بمعالجة معاملة باعتباره المستخدم الضحية (ب) من خلال التلاعب أو إعادة إعداد الجلسة أو حالة المعاملة أو هوية المستخدم أو المعاملة.
٣-١٢	التحقق من أن التطبيق لا يسمح بالتلاعب بمعايير قواعد العمل عالية القيمة والتي تشمل، على سبيل المثال لا الحصر، السعر، والفائدة، والخصومات، والمعلومات القابلة لتحديد الهوية (PII)، والأرصدة، وهويات الأسهم، وغيرها.
٤-١٢	التحقق من وجود إجراءات دفاعية في التطبيق للحماية من هجمات الإنكار، حيث تشمل هذه الإجراءات سجلات المعاملات المحمية والقابلة للتحقق، وسجلات التدقيق أو سجلات النظام، وفي الأنظمة ذات القيمة الأعلى، المراقبة المباشرة لأنشطة المستخدم والمعاملات بحثاً عن أي أنشطة غير طبيعية.

١٢	قواعد العمل (Business Logic)
١٢-٥	التحقق من أن التطبيق يوفر الحماية من هجمات الإفصاح عن المعلومات مثل مرجعيات الكائنات المباشرة، والتلاعب، واستخدام الهجمات التخمينية لاختراق الجلسة، وأنواع الهجمات الأخرى.
١٢-٦	التحقق من وجود ضوابط كشف وضبط كافية في التطبيق للحماية من الهجمات التخمينية (مثل الاستخدام المستمر لدالة معينة) أو هجمات حجب الخدمة.
١٢-٧	التحقق من وجود ضوابط وصول كافية في التطبيق لمنع هجمات رفع مستوى المزايا والصلاحيات، وتشمل هذه الضوابط منع المستخدمين المجهولين من الوصول إلى البيانات المحمية أو الدالات المحمية، أو منع المستخدمين من الوصول إلى معلومات المستخدمين الآخرين، أو استخدام وظائف ذات مزايا وصلاحيات هامة وحساسة.
١٢-٨	التحقق من أن التطبيق يعالج دفعات قواعد العمل في خطوات متتالية فقط، بحيث تتم معالجة كافة الخطوات مباشرة، وتجنب المعالجة بطريقة غير منتظمة أو التجاوز عن أي خطوات، أو معالجة خطوات مستخدم آخر أو المعاملات المقدمة بسرعة.
١٢-٩	التحقق من أن التطبيق يتضمن تصاريح وصلاحيات إضافية (مثل تحقق الإعداد أو التحقق من الهوية المتغير) لأنظمة القيم المتدنية و/أو فصل المهام للتطبيقات ذات القيم المرتفعة لإنفاذ ضوابط مكافحة الاحتيال وفقاً لمخاطر التطبيق وعمليات الاحتيال السابقة.
١٢-١٠	التحقق من أن للتطبيق حدود عمل يطبقها في موقع موثوق (كتطبيقها على خادم محمي) على كل مستخدم أو بشكل يومي، والتي تتضمن تنبيهات قابلة للإعداد واستجابات تلقائية للهجمات التلقائية أو غير الاعتيادية.

يستعرض الجدول التالي: (جدول رقم: ٢٦ - الملفات والمصادر) إجراءات التحقق من المكونات التي تحتوي ثغرات معروفة.

١٣	الملفات والمصادر (OWASP:A9:2017 - استخدام المكونات التي تحتوي ثغرات معروفة) Files and Resources (OWASP:A9:2017 – Using Components with Known Vulnerabilities)
١٣-١	التحقق من أن إعادة التوجيه والإرسال في شريط العنوان (URL) لا تتضمن بيانات غير مصرحة.
١٣-٢	التحقق من توحيد أسماء الملفات وبيانات المسارات التي يتم الحصول عليها من مصادر غير موثوقة لإلغاء هجمات تجاوز المسار.
١٣-٣	التحقق من فحص الملفات التي يتم الحصول عليها من مصادر غير موثوقة من خلال برامج مكافحة الفيروسات لمنع تحميل برمجيات خبيثة معروفة.
١٣-٤	التحقق من عدم استخدام المعايير التي تم الحصول عليها من مصادر غير موثوقة للتلاعب في أسماء الملفات أو أسماء المسارات أو ملفات وكائنات النظام دون توحيدها أولاً والتحقق من مدخلاتها لمنع هجمات إدراج الملفات المحلية.
١٣-٥	التحقق من توحيد المعايير التي تم الحصول عليها من مصادر غير موثوقة والتحقق من مدخلاتها وترميز مخرجاتها لمنع هجمات إدراج الملفات عن بعد، خصوصاً عندما يكون من الممكن تنفيذ المدخلات مثل العناوين أو المصادر أو إدراج القوالب.
١٣-٦	التحقق من عدم السماح بإدراج محتوى عشوائي عن بعد عند مشاركة موارد "IFRAMEs" و"HTML 5" عبر النطاقات.
١٣-٧	التحقق من تخزين الملفات التي تم الحصول عليها من مصادر غير موثوقة خارج "Webroot".
١٣-٨	التحقق من إعداد وضبط خادم الويب أو التطبيق تلقائياً لحجب الوصول إلى المصادر البعيدة أو الأنظمة خارج خادم الويب أو التطبيق.
١٣-٩	التحقق من أن شفرة التطبيق لا تنفذ بيانات مرفوعة تم الحصول عليها من مصادر غير موثوقة.
١٣-١٠	التحقق من ضبط إعدادات مشاركة مصادر تطبيقات "Flash" أو "Silverlight" أو غيرها من تطبيقات الإنترنت الغنية (RIA) عبر النطاقات بحيث تمنع الوصول غير المصرح به أو الوصول عن بعد غير المعتمد.
١٣-١١	التحقق من أن كافة أنواع الملفات المسموح برفعها مقتصرة على غايات العمل وحسب الحاجة (مثل ملفات "PDF" ومستندات برامج "Office").
١٣-١٢	التأكد من أن التحقق من نوع الملف يتم من خلال التحقق من عناوين الملفات وليس من خلال اسم امتداد الملفات فقط.

١٣	الملفات والمصادر (OWASP:A9:2017 - استخدام المكونات التي تحتوي ثغرات معروفة) Files and Resources (OWASP:A9:2017 – Using Components with Known Vulnerabilities)
١٣-١٣	التحقق من عدم تفعيل امتيازات وصلاحيات التنفيذ في أدلة تحميل الملفات.
١٣-١٤	التحقق من ضبط إعدادات ملفات ومصادر التطبيق تلقائياً على وضعية القراءة فقط.
١٣-١٥	التحقق من إلغاء كافة أنواع المشاركات والمشاركات الإدارية غير اللازمة، وتقييد الوصول إلى المشاركات أو جعله يتطلب التحقق من الهوية.
١٣-١٦	طلب التحقق من الهوية قبل السماح برفع الملفات.
١٣-١٧	وضع حد على حجم الملفات التي يمكن رفعها والذي يجب ألا يتجاوز الحجم المطلوب لغايات العمل (على سبيل المثال، ١ ميغابايت كحد أعلى)، وإضافة ملاحظة على صفحة الويب تخص أحجام الملفات المقبولة.

يظهر الجدول التالي: (جدول رقم: ٢٧ - التحقّق من الهاتف المحمول) إجراءات التحقق من أمن إعدادات تطبيقات الهواتف المحمولة والأجهزة الذكية.

١٤	التحقّق من الهاتف المحمول (Mobile Verification)
١٤-١	التأكد من تحقق العميل من شهادات تشفير طبقة المنافذ الآمنة (SSL).
١٤-٢	التحقق من عدم استخدام قيم رقم تعريف الجهاز المميز (UDID) كضوابط أمنية.
١٤-٣	التحقق من أن تطبيق الهاتف المحمول لا يخزن المعلومات المحمية على المصادر المشتركة على الجهاز (مثل بطاقة "SD" أو المجلدات المشتركة).
١٤-٤	التحقق من أن المعلومات المحمية ليست مخزنة في قاعدة بيانات "SQLite" على الجهاز.
١٤-٥	التحقق من أن المفاتيح السرية وكلمات المرور ليست مثبتة في الشفرة في البرامج التنفيذية.
١٤-٦	التحقق من أن تطبيق الهاتف المحمول يمنع تسرب المعلومات المحمية عن طريق خاصية التصوير التلقائي في نظام تشغيل "iOS".
١٤-٧	التحقق من أن التطبيق لا يمكن تشغيله على جهاز تم إلغاء القيود الموجودة عليه (Jailbroken) أو جهاز يتمتع بصلاحيات ومزايا هامة وحساسة (Rooted).
١٤-٨	التحقق من أن وقت انتهاء الجلسة له قيمة منطقية.
١٤-٩	التحقق من التصاريح التي يتم طلبها ومن المصادر التي يتم منح تصاريح الوصول إليها (AndroidManifest.xml، وiOS Entitlements).
١٤-١٠	التحقق من أن سجلات انهيار النظام لا تتضمن معلومات محمية.
١٤-١١	التحقق من عدم وضوح النظام الثنائي في التطبيق.
١٤-١٢	التحقق من أن كافة بيانات الاختبار قد تم إزالتها من حاوية التطبيق (.ipa .bar .apk).
١٤-١٣	التحقق من أن التطبيق لا يقوم بتسجيل المعلومات المحمية على سجل النظام أو ملفات النظام.
١٤-١٤	التحقق من أن التطبيق لا يتيح الإكمال التلقائي للنصوص الحساسة في حقول المدخلات مثل حقول كلمات المرور أو المعلومات الشخصية أو بطاقات الائتمان.
١٤-١٥	التحقق من أن تطبيق الهاتف المحمول يطبق عملية تثبيت الشهادات (Certificate Pinning) لمنع إدارة حركة البيانات في التطبيق بالوكالة.
١٤-١٦	التحقق من عدم وجود إعدادات خاطئة في ملفات الإعدادات (مجموعة العلامات التصحيحية، وتصاريح قابلة للقراءة وللكتابة العالمية).
١٤-١٧	التحقق من تحديث مكتبات الأطراف الخارجية قيد الاستخدام وعدم احتوائها على أي ثغرات معروفة.
١٤-١٨	التحقق من عدم تخزين بيانات الويب مثل حركة بيانات بروتوكول نقل النص التشعبي الآمن (HTTPS).
١٤-١٩	التحقق من عدم استخدام سلسلة الأحرف للاستفسار (Query String) مع المعلومات المحمية. بدلاً من ذلك، يجب استخدام طلب "POST" عبر طبقة المنافذ الآمنة (SSL) مع رمز تعريفي للحماية من تزوير الطلب عبر المواقع (CSRF).

١٤	التحقّق من الهاتف المحمول (Mobile Verification)
١٤-٢٠	التحقق، إن أمكن، من أن أرقام الحسابات الشخصية متقطعة قبل تخزينها على الجهاز.
١٤-٢١	التحقق من أن التطبيق يستفيد من خاصية التوزيع العشوائي لمخطط مساحات العناوين (ASLR).
١٤-٢٢	التحقق من أن البيانات المسجلة عن طريق لوحة المفاتيح (iOS) لا تتضمن بيانات اعتماد أو معلومات مالية أو معلومات محمية أخرى.
١٤-٢٣	في تطبيقات الأندرويد، التحقق من أن التطبيق لا ينشئ ملفات بتصاريح "MODE_WORLD_READABLE " أو " MODE_WORLD_WRITABLE".
١٤-٢٤	التحقق من تخزين المعلومات المحمية بطريقة مشفرة وآمنة (حتى عند تخزينها في سلسلة مفاتيح "iOS").
١٤-٢٥	التحقق من تطبيق آليات مكافحة التصحيح والهندسة العكسية في التطبيق.
١٤-٢٦	التحقق من أن التطبيق لا يستورد أنشطة حساسة أو مزودي محتوى أو غيرهم على الأندرويد.
١٤-٢٧	التحقق من استخدام هيكليات متغيرة لسلاسل الحروف العشوائية (Strings) الحساسة مثل أرقام الحسابات، والكتابة فوقها عند عدم استخدامها (لتقليل الأضرار الناجمة عن هجمات تحليل الذاكرة).
١٤-٢٨	التأكد من تنفيذ التحقق الكامل من البيانات على المدخلات لأي رسائل أنشطة ومزودي محتوى ومتلقي بث معرضين للمخاطر (الأندرويد).

يستعرض الجدول التالي: (جدول رقم: ٢٨ - أمن قواعد البيانات) إجراءات التحقق من الإعدادات الأمنية الخاطئة لقواعد البيانات والتطبيقات.

١٥	أمن قواعد البيانات (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة) Database Security (OWASP:A6:2017 – Security Misconfiguration)
١٥-١	التحقق من استخدام الاستفسارات المضبوطة بمعايير لمنع حقن تعليمات الاستعلام البنيوية (SQL Injection).
١٥-٢	التحقق من استخدام بيانات اعتماد معقدة وآمنة للوصول إلى قواعد البيانات.
١٥-٣	التحقق من أن التطبيق الذي يصل إلى قواعد البيانات يمتلك أدنى مستوى ممكن من الامتيازات والصلاحيات المطلوبة.
١٥-٤	التحقق من أن سلاسل الحروف العشوائية (Strings) للاتصال ليست مثبتة في الشفرة ضمن التطبيق، خصوصاً بيانات اعتماد التحقق من الهوية من قاعدة البيانات.
١٥-٥	التحقق من إغلاق الاتصال بقاعدة البيانات بأسرع ما يمكن.
١٥-٦	التحقق من حذف كافة وظائف قاعدة البيانات غير اللازمة أو غير المستخدمة أو إلغاء تفعيلها، بما في ذلك محتوى المورد التلقائي، وتثبيت الحد الأدنى من الخصائص والخيارات اللازمة لعمل التطبيق. على سبيل المثال، إلغاء تفعيل الإجراءات أو الخدمات المخزنة وحزم الخصائص المفيدة غير اللازمة.
١٥-٧	التحقق من إلغاء تفعيل أي حسابات تلقائية أو غير ضرورية والتي يمكن من خلالها الوصول إلى قواعد البيانات غير اللازمة لدعم متطلبات الأعمال.
١٥-٨	التحقق من أن التطبيق يستخدم بيانات اعتماد مختلفة لكل ميزة وصلاحية (مثل مستخدم، ومستخدم للقراءة فقط، وضيف، ومشرفين) عند اتصاله بقاعدة البيانات.
١٥-٩	التحقق من إلغاء تفعيل تسجيل الدخول عن بعد والجلسات المجهولة إذا لم يكن هناك حاجة إليها.
١٥-١٠	بالنسبة للتطبيقات التي تعتمد على قاعدة بيانات، يجب استخدام قوالب الإعداد والتحصين الموحدة، واختبار جميع الأنظمة التي تعتبر جزءاً من إجراءات العمل الحساسة.

الأدوار والمسؤوليات

- **راعي ومالك وثيقة المعيار: إدارة الأمن السيبراني .**
- **مراجعة المعياروتحديثه: إدارة الأمن السيبراني.**
- **تنفيذ المعياروتطبيقه: إدارة الأمن السيبراني .**

الالتزام بالمعيار

- يجب على إدارة الأمن السيبراني وبناءً على موافقة صاحب الصلاحية معالي رئيس الجامعة التأكد وبصفة دورية من التزام كافة جهات الجامعة بتطبيق هذا المعيار.
- يجب على منسوبي جامعة الملك فيصل الالتزام بهذا المعيار.
- قد يُعرّض أي انتهاك لهذا المعيار والمعايير ذات الصلة بالأمن السيبراني صاحب المخالفة إلى إجراء نظامي حسب الإجراءات النظامية المتبعة في الجامعة و/أو حسب الإجراءات النظامية الصادرة من الجهات ذات العلاقة.

القسم الرابع

قاموس المصطلحات والملاحق

ا- قاموس المصطلحات

م	المصطلح	وصف المصطلح
١	الأمن السيبراني Cybersecurity	حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية؛ ومكوناتها من عتاد وبرمجيات: وما تقدمه من خدمات: وما تحويه من بيانات، من أي اختراق؛ أو تعطيل؛ أو تعديل؛ أو دخول؛ أو استخدام: أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات؛ والأمن الإلكتروني؛ والأمن الرقمي ونحو ذلك.
٢	الفضاء السيبراني Cyberspace	الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت، وشبكات الاتصالات، وأنظمة الحاسب، والأجهزة المتصلة بالإنترنت؛ إلى جانب العتاد وأجهزة التحكم المرتبطة بها.
٣	التوافر Availability	ضمان إمكانية الوصول والاستخدام عند الطلب، من مستخدم أو إجراء أو نظام مصرح له بشكل يعتمد عليه.
٤	السلامة Integrity	الحماية ضد تعديل المعلومات أو تخريبها بشكل غير مصرح به، كما تشمل ضمان عدم الإنكار للمعلومات والأصالة.
٥	السرية Confidentiality	خاصية عدم الإفصاح عن المعلومات لمستخدم أو إجراء أو نظام غير مصرح له إلا في حال وجود تصريح لهم للوصول إليها.
٦	توكيد المعلومات Information Assurance	التدابير التي تحمي المعلومات، وأنظمة المعلومات، من خلال ضمان توافرها وسلامتها وأصالتها، وعدم الإنكار للمعلومات وسريتها.
٧	المسؤولية Accountability	القدرة على تتبع مسار نشاط أو حدث معين حتى الوصول إلى الطرف المسؤول؛ منشئ النشاط. ويدعم ذلك عدم الإنكار، تشخيص الخطأ، اكتشاف ومنع التسللات، وإجراءات ما بعد الاكتشاف كالتعافي والإجراءات القانونية.
٨	التحقق من الهوية Authentication	التأكد من هوية المستخدم، أو العملية، أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد التقنية. وليس له علاقة بتحديد حقوق الوصول للموارد والأصول التقنية.
٩	التحقق من الهوية متعدد العناصر Multi-Factor Authentication	نظام أمني يتحقق من هوية المستخدم، يتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر: - المعرفة؛ شيء يعرفه المستخدم، مثل: كلمة المرور. - الحيازة؛ شيء يملكه المستخدم، مثل: برنامج أو جهاز توليد أرقام عشوائية أو رسائل قصيرة مؤقتة لتسجيل الدخول، ويطلق عليها One-time passwords - الملازمة؛ صفة أو سمة حيوية متعلقة بالمستخدم نفسه فحسب، مثل: بصمة الإصبع.
١٠	التصريح Authorization	تعريف حقوق/تراخيص الوصول إلى الموارد والأصول المعلوماتية والتقنية للجهة بشكل عام، والتحكم بمستويات الوصول على وجه الخصوص، والتأكد منها.
١١	أصل Asset	الموارد الملموسة، أو غير الملموسة، ذات قيمة للجهة. بما في ذلك الموظفين والتقنيات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات، والمعلومات والخصائص، مثل: سمعة الجهة وهويتها وقدراتها المعرفية أو المهنية.
١٢	التشفير Cryptography	القواعد التي تشتمل على مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به والتعديل غير المكتشفة بحيث لا يمكن للأشخاص غير المعنيين قراءتها ومعالجتها.
١٣	صمود الأمن السيبراني Cybersecurity Resilience	القدرة الشاملة للجهة على التصدي للحوادث السيبرانية وامتصاص الأضرار والتعافي منها في الوقت المناسب.
١٤	دفاع أمني متعدد المستويات Defense-in-Depth	مفهوم يُعنى بوضع مستويات دفاعية متعددة من الضوابط الأمنية وذلك بالتكامل بين الأشخاص، التقنية، والقدرات التشغيلية.
١٥	هجوم سيبراني Cyber Attack	استغلال غير مشروع لأنظمة الحاسب، والشبكات، والمنظمات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية؛ بهدف إحداث أضرار. وتشمل أي نوع من الأنشطة الخبيثة التي تحاول الوصول غير المشروع، أو تعطيل، أو منع، أو تدمير موارد النظم المعلوماتية، أو المعلومات نفسها.
١٦	هجمات حجب الخدمة الموزعة Distributed Denial of Service Attack	هي محاولة لتعطيل النظام، وجعل خدماته غير متوافرة؛ عن طريق إرسال طلبات كثيرة من أكثر من مصدر في الوقت نفسه.
١٧	رسائل التصيّد الإلكتروني Phishing Email	التنكر على هيئة جهة جديرة بالثقة عن طريق رسائل بريد إلكترونية للحصول على معلومات حساسة، مثل أسماء المستخدمين، وكلمات المرور، أو تفاصيل بطاقة الائتمان، وذلك لأسباب ونوايا ضارة وخبيثة.
١٨	المعلومات الاستباقية للتهديدات Threat Intelligence	معلومات منظمة قد تم تحليلها حول الهجمات الأخيرة، والحالية، والمحتملة، والتي يمكن أن تشكل تهديداً سيبرانياً للمنظمة.
١٩	مشاركة المعلومات Information Sharing	تبادل البيانات والمعلومات، أو المعرفة - أو كليهما - لاستخدامها في إدارة المخاطر والتهديدات أو الاستجابة للأحداث السيبرانية.

م	المصطلح	وصف المصطلح
٢٠	البرمجيات الضارة Malware	برنامج يصيب الأنظمة بطريقة خفية (في الغالب) بغاية انتهاك سرية، أو سلامة، أو توافر بيانات الضحية، أو تطبيقاته، أو نظم التشغيل الخاصة به.
٢١	برمجيات الفدية Ransomware	برمجيات ضارة تجعل بيانات وأنظمة الضحية غير قابلة للاستخدام لحين دفعه لمبلغ مالي.
٢٢	التعافي من الكوارث Disaster Recovery	الأنشطة والبرامج والخطط المصممة؛ لإرجاع الوظائف وخدمات الأعمال الحساسة للجهة؛ إلى حالتها الطبيعية، وذلك بعد التعرض إلى هجمات سيبرانية، أو تعطل لهذه الخدمات والوظائف.
٢٣	جدار الحماية Firewall	عتاد أو برمجيات، تحد من حركة مرور بيانات الشبكة؛ وفقًا لمجموعة من قواعد تمكين الوصول، التي تحكم ما هو مسموح ومصرح به؛ من عدمه.
٢٤	ثغرة Vulnerability	أي نوع من نقاط الضعف في نظام الحاسب أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، مما يجعل الأمن السيبراني عرضة للتهديد.
٢٥	تقييم الثغرات Vulnerability Assessment	عملية فحص ممنهجة لنظم المعلومات أو التطبيقات لتحديد مستوى الضوابط الأمنية، وتحديد أوجه القصور فيها، وتوفير البيانات التي يمكن من خلالها التنبؤ بفعالية الضوابط الأمنية، والتأكد من كفاءتها بعد التنفيذ.
٢٦	اختبار الاختراق Penetration Testing	عملية اختبار نظام، أو شبكة، أو موقع إلكتروني، أو تطبيق هواتف ذكية؛ للكشف عن ثغرات، يمكن أن تُستغل لتنفيذ اختراق سيبراني.
٢٧	بروتوكول الإشارة الضوئية (TLP)	يستخدم نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية): أحمر – شخصي وسري للمستلم فقط، برتقالي – مشاركة محدودة، أخضر – مشاركة في نفس المجتمع، أبيض – غير محدود.
٢٨	الضابط رقم ١-١-٥ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) للجهة."
٢٩	الضابط رقم ١-٢-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب إنشاء لجنة إشرافية للأمن السيبراني بتوجيه من صاحب الصلاحية للجهة لضمان التزام ودعم ومتابعة تطبيق برامج وتشريعات الأمن السيبراني، ويتم تحديد وتوثيق واعتماد أعضاء اللجنة ومسؤولياتها وإطار حوكمة أعمالها على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها. ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه، مع الأخذ بالاعتبار عدم تعارض المصالح."
٣٠	الضابط رقم ١-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد سياسات وإجراءات الأمن السيبراني وما تشمله من ضوابط ومتطلبات الأمن السيبراني، وتوثيقها واعتمادها من قبل صاحب الصلاحية في الجهة، كما يجب نشرها إلى ذوي العلاقة من العاملين في الجهة والأطراف المعنية بها."
٣١	الضابط رقم ١-٣-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب أن تكون سياسات وإجراءات الأمن السيبراني مدعومة بمعايير تقنية أمنية (على سبيل المثال: المعايير التقنية الأمنية لجدار الحماية وقواعد البيانات، وأنظمة التشغيل، إلخ)."
٣٢	الضابط رقم ١-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب على صاحب الصلاحية تحديد وتوثيق واعتماد الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للجهة، وتكليف الأشخاص المعنيين بها، كما يجب تقديم الدعم اللازم لإنفاذ ذلك، مع الأخذ بالاعتبار عدم تعارض المصالح."
٣٣	الضابط رقم ١-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة. وذلك وفقًا لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية."
٣٤	الضابط رقم ١-٦-٢-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"اجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين المشاريع والتغييرات."
٣٥	الضابط رقم ١-٦-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"استخدام معايير التطوير الآمن للتطبيقات (Secure Coding Standards)."
٣٦	الضابط رقم ١-٦-٣-٥ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"اجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين التطبيقات."
٣٧	الضابط رقم ١-٧-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب على الجهة الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني."

م	المصطلح	وصف المصطلح
٣٨	الضابط رقم ١-٨-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمن السيبراني دوريًا."
٣٩	الضابط رقم ١-٨-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني في الجهة، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني (مثل الإدارة المعنية بالمراجعة في الجهة). على أن تتم المراجعة والتدقيق بشكل مستقل يراعى فيه مبدأ عدم تعارض المصالح، وذلك وفقًا للمعايير العامة المقبولة للمراجعة والتدقيق والمتطلبات التشريعية والتنظيمية ذات العلاقة."
٤٠	الضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم في الجهة."
٤١	الضابط رقم ٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"التأكد من أن الجهة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية، والتقنية للجهة، ودقتها، وتوافرها."
٤٢	الضابط رقم ٢-١-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد ونشر سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة."
٤٣	الضابط رقم ٢-٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة."
٤٤	الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة."
٤٥	الضابط رقم ٢-٣-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على أجهزة المستخدمين والخوادم باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن."
٤٦	الضابط رقم ٢-٣-٣-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"إدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات والأجهزة (Patch Management)."
٤٧	الضابط رقم ٢-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة."
٤٨	الضابط رقم ٢-٤-٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail)."
٤٩	الضابط رقم ٢-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة."
٥٠	الضابط رقم ٢-٨-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني للتشفير في الجهة."
٥١	الضابط رقم ٢-٩ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"ضمان حماية بيانات ومعلومات الجهة والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.:
٥٢	الضابط رقم ٢-١٠-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجهة."

م	المصطلح	وصف المصطلح
٥٣	الضابط رقم ٢-١١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجهة."
٥٤	الضابط رقم ٢-١٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة."
٥٥	الضابط رقم ٢-١٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة."
٥٦	الضابط رقم ٢-١٤ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"ضمان حماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب."
٥٧	الضابط رقم ٢-١٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية."
٥٨	الضابط رقم ٤-١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجهة."
٥٩	الضابط رقم ٤-١-٢ من الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018)	"يجب أن تغطي متطلبات الأمن السيبراني ضمن العقود والاتفاقيات (مثل اتفاقية مستوى الخدمة SLA) مع الأطراف الخارجية التي قد تتأثر بإصابتها بيانات الجهة أو الخدمات المقدمة لها."
٦٠	(ECC-2-5-3-1) - الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن، واللازم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة، باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth)."
٦١	(ECC-2-5-3-8) - الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.
٦٢	(ECC-2-11-3-1) - الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"نطاق عمل اختبار الاختراق، ليشمل جميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، المواقع الالكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الإلكتروني والدخول عن بعد."
٦٣	(ECC-4-1-3-2) - الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة، والتي تستخدم طريقة الوصول عن بعد، موجودة بالكامل داخل المملكة."
٦٤	(CSCC-2-12-2) - الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للجهة."
٦٥	(ECC-2-15-3-1) - الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall)."
٦٦	(ECC-2-15-3-2) - الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture)."
٦٧	(ECC-2-15-3-3) - الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"استخدام بروتوكولات آمنة (مثل بروتوكول HTTPS)."
٦٨	(ECC-2-9-2) - الضوابط الأساسية للأمن السيبراني (ECC-1:2018)	"يجب تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة."
٦٩	(CSCC-1-2-1-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"تنفيذ إجراء تقييم مخاطر الأمن السيبراني، على الأنظمة الحساسة، مرة واحدة سنوياً، على الأقل."
٧٠	(CSCC-2-3-1-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج؛ للعمل على الخوادم الخاصة بالأنظمة الحساسة."

م	المصطلح	وصف المصطلح
٧١	(CSCC-2-3-1-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"حماية الخوادم الخاصة بالأنظمة الحساسة بتقنيات حماية الأجهزة الطرفية(End-point Protection) المعتمدة لدى الجهة."
٧٢	(CSCC-2-3-1-6) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"مراجعة إعدادات الأنظمة الحساسة وتحصيناتها (Secure Configuration and Hardening) كل ستة أشهر على الأقل."
٧٣	(CSCC-2-2-1-7) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"الإدارة الآمنة لحسابات الخدمات ((Service Account ما بين التطبيقات والأنظمة؛ وتعطيل الدخول البشري التفاعلي (Interactive login) من خلالها."
٧٤	(CSCC-2-2-1-8) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"فيما عدا مشرفي قواعد البيانات (Database Administrators)، يمنع الوصول أو التعامل المباشر لأي مستخدم مع قواعد البيانات؛ ويتم ذلك من خلال التطبيقات فقط، وبناءً على الصلاحيات المخوّل بها؛ مع مراعاة تطبيق حلول أمنية تحد، أو تمنع من اطلاع مشرفي قواعد البيانات على البيانات المصنفة (Classified Data)."
٧٥	(CSCC-2-3-1-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج؛ للعمل على الخوادم الخاصة بالأنظمة الحساسة."
٧٦	(CSCC-2-3-1-3) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"تطبيق حزم التحديثات، والإصلاحات الأمنية، مرة واحدة شهرياً على الأقل، للأنظمة الحساسة الخارجية، والمتصلة بالإنترنت؛ وكل ثلاثة أشهر على الأقل، للأنظمة الحساسة الداخلية؛ مع اتباع آليات التغيير المعتمدة لدى الجهة."
٧٧	(CSCC-2-4-1-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"مراجعة إعدادات جدار الحماية (Firewall rules) وقوائمه؛ كل ستة أشهر، على الأقل."
٧٨	(CSCC-2-4-1-3) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"منع التوصيل المباشر، لأي جهاز بالشبكة المحلية للأنظمة الحساسة؛ إلا بعد الفحص، والتأكد من توافر عناصر الحماية المحققة، للمستويات المقبولة للأنظمة الحساسة."
٧٩	(CSCC-2-4-1-6) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"منع الأنظمة الحساسة من الاتصال بالإنترنت في حال أن كانت تقدم خدمة داخلية للجهة؛ ولا توجد هناك حاجة ضرورية جداً، للدخول على الخدمة من خارج الجهة."
٨٠	(CSCC-2-4-1-8) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") للحد من المخاطر الناتجة عن هجمات تعطيل الشبكات."
٨١	(CSCC-2-5-1-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"منع الوصول من الأجهزة المحمولة للأنظمة الحساسة، إلا لفترة مؤقتة فقط؛ وذلك بعد إجراء تقييم المخاطر، وأخذ الموافقات اللازمة من الإدارة المعنية بالأمن السيبراني في الجهة."
٨٢	(CSCC-2-5-1-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"تشفير أقراص الأجهزة المحمولة، ذات صلاحية الوصول للأنظمة الحساسة، تشفيراً كاملاً (Full Disk Encryption)."
٨٣	(CSCC-2-6-1-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"عدم استخدام بيانات الأنظمة الحساسة في غير بيئة الإنتاج (Production Environment) إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل: تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling)."
٨٤	(CSCC-2-6-1-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"تصنيف جميع بيانات الأنظمة الحساسة."
٨٥	(CSCC-2-6-1-5) - ضوابط الأمن السيبراني للأنظمة الحساسة :1-CSCC (2019	"منع نقل أي من بيانات بيئة الإنتاج الخاصة بالأنظمة الحساسة إلى أي بيئة أخرى."

م	المصطلح	وصف المصطلح
٨٦	(CSCC-2-7-1-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"تشفير جميع بيانات الأنظمة الحساسة؛ أثناء النقل (Data-In-Transit)."
٨٧	(CSCC-2-7-1-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"تشفير جميع بيانات الأنظمة الحساسة؛ أثناء التخزين (Data-At-Rest) على مستوى الملفات، أو قاعدة البيانات، أو على مستوى أعمدة محددة، داخل قاعدة البيانات."
٨٨	(CSCC-2-7-1-3) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وآمنة وفقاً لما تصدره الهيئة بهذا الشأن."
٨٩	(CSCC-2-8-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"يجب أن تغطي متطلبات الأمن السيبراني إدارة النسخ الاحتياطية."
٩٠	(CSCC-2-8-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"يجب إجراء فحص دوري؛ كل ثلاثة أشهر على الأقل، لتحديد مدى فعالية استعادة النسخ الاحتياطية، الخاصة بالأنظمة الحساسة."
٩١	(CSCC-2-9-1-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"تقييم الثغرات ومعالجتها (بتنصيب حزم التحديثات والإصلاحات) على المكونات التقنية للأنظمة الحساسة، مرة واحدة شهرياً، على الأقل، للأنظمة الحساسة الخارجية، والمتصلة بالإنترنت؛ وكل ثلاثة أشهر على الأقل، للأنظمة الحساسة الداخلية."
٩٢	(CSCC-2-9-1-3) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"معالجة فورية للثغرات الحرجة (Critical Vulnerabilities) المكتشفة حديثاً؛ مع اتباع آليات إدارة التغيير، المعتمدة لدى الجهة."
٩٣	(CSCC-2-10-1-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"نطاق عمل اختبار الاختراق، ليشمل جميع المكونات التقنية للأنظمة الحساسة، وجميع الخدمات المقدمة داخلياً وخارجياً."
٩٤	(CSCC-2-10-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"يجب عمل اختبار الاختراق على الأنظمة الحساسة، كل ستة أشهر؛ على الأقل."
٩٥	(CSCC-2-12-1-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"الإدارة الآمنة للجلسات (Secure Session Management)، وتشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout)."
٩٦	(CSCC-2-12-1-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"تطبيق معايير أمن التطبيقات وحمايتها (OWASP Top Ten) في حدها الأدنى."
٩٧	(CSCC-2-12-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"يجب استخدام مبدأ المعمارية ذات المستويات المتعددة (Multi-tier Architecture) على ألا يقل عدد المستويات عن ٣ (٣-Tier Architecture)."
٩٨	(CSCC-4-1-1-1) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة العاملين على الأنظمة الحساسة."
٩٩	(CSCC-4-1-1-2) - ضوابط الأمن السيبراني للأنظمة الحساسة :CSCC–1 (2019	"أن تكون خدمات الإسناد، والخدمات المدارة على الأنظمة الحساسة؛ عن طريق شركات، وجهات وطنية؛ وفقًا للمتطلبات التشريعية، والتنظيمية ذات العلاقة."

٢- الملاحق

- وثيقة الضوابط الأساسية للأمن السيبراني (Essential Cybersecurity Controls – ECC – 1 : 2018)، صادرة من الهيئة الوطنية للأمن السيبراني – رابط الاطلاع على الوثيقة: https://nca.gov.sa/files/ecc-ar.pdf .
- وثيقة ضوابط الأمن السيبراني للأنظمة الحساسة (Controls Cybersecurity Systems Controls – CSCC – 1 : 2019)، صادرة من الهيئة الوطنية للأمن السيبراني – رابط الاطلاع على الوثيقة: https://nca.gov.sa/files/cscc-ar.pdf .
- قاموس مصطلحات الأمن السيبراني، صادر من الهيئة الوطنية للأمن السيبراني - الرابط: https://nca.gov.sa/pages/glossary.html .
- نماذج سياسات الأمن السيبراني Cybersecurity Toolkit، صادرة من الهيئة الوطنية للأمن السيبراني - رابط النماذج: https://nca.gov.sa/pages/kit.html .
- وثيقة سياسات حوكمة البيانات (تصنيف البيانات –حماية البيانات الشخصية –مشاركة البيانات الشخصية –حرية المعلومات البيانات المفتوحة –نمذجة وهيكلة البيانات –مرجعية البيانات والإشراف عليها –أمن البيانات وحمايتها –التخزين والإستيفاء). https://www.kfu.edu.sa/ar/Departments/StrategicPlans/Pages/%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9%20%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9%20%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%A7%D8%AA.aspx

- نهاية الوثيقة -

KFU

جامعة الملك فيصل

KING FAISAL UNIVERSITY

جـامعة ووطـن.. نمـاء.. واســتدامة..

www.kfu.edu.sa