KFU
جامعة الملك فيصل
KING FAISAL UNIVERSITY
جـامعة ووطـن .. نمـاء .. واسـتدامة ..

سياسة الاستخدام الآمن

للتطبيقات والخدمات الإلكترونية

KFU
جامعة الملك فيصل
KING FAISAL UNIVERSITY
جـامعة ووطـن..نمـاء..واســتدامة..

مقدمة

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.

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:

1. 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.
2. 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.
3. 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.

KFU
جامعة الملك فيصل
KING FAISAL UNIVERSITY
جـامعة ووطـن..نمـاء..واســتدامة..

4. 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.
5. يُمنع على المستخدم استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.
6. 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.
7. يجب على المستخدم استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.
8. يجب على المستخدم إبلاغ الجهة المعنية بالأمن السيبراني بالجامعة في حال وجود مواقع مشبوهة ينبغي حجبها.
9. يُمنع على المستخدم استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.
10. يُمنع على المستخدم أي سرقة للموارد بما في ذلك المعلومات الحساسة.
11. يُمنع على المستخدم القيام بتزوير أو انتحال هوية الغير أو تغيير هويته وذلك عند استخدام التطبيقات والخدمات الإلكترونية الخاصة بالجامعة.
12. يُمنع على المستخدم تنزيل البرمجيات والأدوات أو تثبيتها على أصول الجامعة دون الحصول على تصريح مسبق من عمادة تقنية المعلومات.
13. يُمنع على المستخدم استخدام شبكة الإنترنت في غير أغراض العمل بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.
14. 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.

KFU
جامعة الملك فيصل
KING FAISAL UNIVERSITY
جـامعة ووطـن..نمـاء..واســتدامة..

15. 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.

16. يُمنع على المستخدم استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من الجهة المعنية بالأمن السيبراني بالجامعة.

17. يُمنع على المستخدم زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

18. يُمنع على المستخدم استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من الجهة المعنية بالأمن السيبراني بالجامعة.

19. 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.

20. يُمنع على المستخدم تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من عمادة تقنية المعلومات.

21. 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.

22. 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.

23. يُمنع على المستخدم تداول رسائل تتضمن محتوى غير لائق أو غير مقبول, بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

24. يجب على المستخدم استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

KFU
جامعة الملك فيصل
KING FAISAL UNIVERSITY
جـامعة ووطـن..نمـاء..واســتدامة..

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

26. يجب على المستخدم تبليغ الجهة المعنية بالأمن السيبراني بالجامعة عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة الجامعة أو أصولها.

27. 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.

28. يُمنع على المستخدم فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

29. 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.

30. 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.

31. يجب على المستخدم تغيير كلمة المرور عند تزويده بكلمة مرور جديدة من قبل مسؤول النظام.

32. يجب على المستخدم عدم إفشاء بيانات حسابه الجامعي أو كلمة المرور للآخرين, وتقع المسؤولية على المستخدم نفسه في المحافظة على كافة بياناته الشخصية.