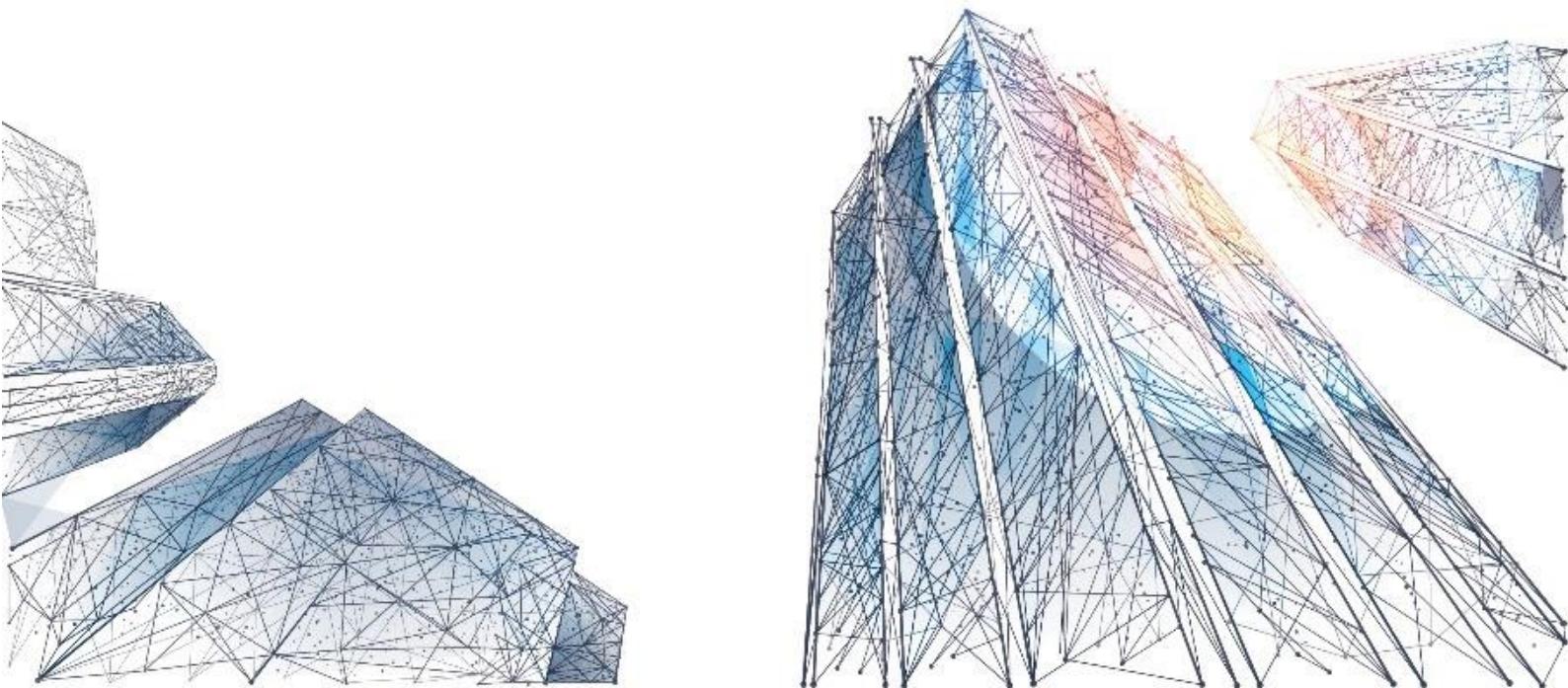
KFU
جامعة الملك فيصل
KING FAISAL UNIVERSITY
جـامعة ووطـن.. نمـاء.. واسـتدامة..

Cybersecurity Policy

at King Faisal University

Dhul-Hijjah 1442H - July 2021

Release: 2.0



Document Information:

Name	Cybersecurity Policy at King Faisal University
pages	120
Current version	2.0
Review &update	At least once a year.
Participation	Allowing participation for King Faisal University employees and related entities
Classification	Restricted - for internal use
Owner	Information Security Unit
Reference	National Cybersecurity Authority

Document History:

Version	Date	Description	Change outlet
0.7	15/11/2020	Creating the document draft	Department of Development and Quality at the Deanship of Information Technology
1.0	13/12/2020	First version	
2.0	12/7/2021	Second version - "Update on the second version "	

Approving List:

Version	Preparation	Review	Approval	Date
1.0	Department of Development and Quality at the Deanship of Information Technology	Information Security Unit at the Deanship of Information Technology	Dean of Information Technology at King Faisal University (Dr. Hasan Shojaa Alkahtani)	24/12/2020
2.0				14/7/2021

Table of Contents

Subject **Page**

List of Tables

Table **Page**

1- Introduction

Cybersecurity protects networks, IT systems, operational technology systems and their components, including the devices and software, and their services and data, from any penetration, disruption, modification, access, use, or illegal exploitation. This concept also includes information security, electronic security, and digital security.

The National Cybersecurity Authority is the regulatory body in the country responsible for preparing and supervising the implementation of the National Cybersecurity Strategy. In addition, it develops policies, governance mechanisms and frameworks, standards, controls, and guidelines related to cybersecurity, generalizes these policies to the relevant entities, and supervises their constant update. It also notifies relevant bodies of the cybersecurity-related risks and threats to protect the vital interests of the kingdom and its national security, sensitive infrastructures and priority sectors, and governmental services and activities. The National Cybersecurity Authority has introduced a range of cybersecurity tools to help the entities develop, upgrade and increase the efficiency of cybersecurity and develop the Cybersecurity Toolkit, which is content that includes illustrative models of the cybersecurity policies, standards, and documents.

The set of cybersecurity tools and models put forward by the National Cybersecurity were taken into account in the establishment of this document. This document aims to provide the policy of cybersecurity at King Faisal University following the regulations and frameworks related to cybersecurity in the country, as well as following modern technologies associated with digital transformation and the subsequent procedures to secure, protect and strengthen all aspects of cybersecurity in the systems and services of King Faisal University.

The present policy included a set of policies and sub-standards related to all aspects of cybersecurity, the organizational structure of cybersecurity at the university and its cybersecurity roles and responsibilities, and the work and functions of the university's Cybersecurity Committee.

2- Policy Objectives

This policy aims at providing cybersecurity requirements based on best practices and standards related to documenting and requirements of cybersecurity to reduce and protect cyber risks from internal and external threats. The protection focuses on the confidentiality, integrity, and availability of information.

The policy complies with the requirements of the regulatory work of King Faisal University and the relevant legislative and regulatory requirements, which is a legislative requirement in regulation No. 1-3-1 of the Basic Controls for Cybersecurity (ECC-1:2018) issued by the National Cybersecurity Authority..

3- Scope and Applicability

This policy covers all the information and technology assets of King Faisal University and applies to all university staff.

This policy is the key to all cybersecurity policies, procedures, and standards of different topics and input to King Faisal University's internal operations, such as human resources operations, supplier management processes, project management processes, change management, etc.

4- Policy Components

1- The Cybersecurity Unit must identify cybersecurity standards, document its policies and programs based on the risk assessment results, and ensure the dissemination of cybersecurity requirements, the commitment of King Faisal University, following the requirements of King Faisal University, and the relevant legislative and regulatory requirements. It should be approved by His Excellency, the President of the University. It should also inform the concerned employees of King Faisal University and related parties about the policy.

2- The Cybersecurity Unit has the right to access information and gather the necessary evidence to ensure the compliance with the relevant legislative and regulatory requirements related to cybersecurity.

3- Cybersecurity Roles and Responsibilities are formed by assigning obvious tasks and responsibilities for all parties involved in the implementation of cybersecurity, including the organizational structure of cybersecurity and the

roles and responsibilities of members of the cybersecurity committee at the university.

4- The Cybersecurity Unit must develop and implement cybersecurity policies, programs, and standards, which include:

4-1 **Cybersecurity Regulatory Compliance Policy** to ensure that the cybersecurity policy and regulations at the university comply with relevant legislative and regulatory requirements.

4-2 **Configuration and Security Policy** to ensure the provision cybersecurity requirements based on best practices and standards through the protection, security and control of the university's information and technical asset settings and applications.

4-3 **Malware Protection Policy** to ensure the provision of cybersecurity requirements based on best practices and standards to protect users' devices, mobile devices, and servers from malware threats and reduce internal and external threats.

4-4 **Server Security Policy** to ensure the provision of cybersecurity requirements based on best practices and standards related to the servers of King Faisal University to reduce cyber risks and protect them from internal and external threats.

4-5 **Networks Security Management Policy** to ensure that university networks are protected from cyber risks.

4-6 **Email Protection policy** to ensure that the university's email is protected from cyber risks.

4-7 **Mobile Devices Security Policy** to ensure that the university's portable devices (including laptops, smartphones, and tablets) are protected from cyber risks and to ensure safe handling and protection of sensitive information during transfer and storage of information and the use of KFU staffs' personal devices ("BYOD").

4-8 **Assets acceptable use** policy to ensure that cybersecurity requirements reduce the cyber risks related the university systems and assets, protect them from internal and external threats, and take care of main protection objectives.

4-9 **Cybersecurity Assessment and Audit Policy** to ensure that the university's cybersecurity controls are implemented and run in accordance with the

university's regulatory policies and procedures, relevant national regulatory legislative requirements, and other regulatory requirements of the university.

4-10 **Identity and Access Management policy** to ensure that cybersecurity protects the logical access to the university's information and technology assets to block unauthorized access and restrict access to complete the business of king Faisal University.

4-11 **Cybersecurity in Human Resources policy** to ensure that cybersecurity risks and requirements of the university employees (employees and contractors) are effectively addressed before, during, and at the end of their work, following the University's regulatory policies and procedures, and related legislative and regulatory requirements.

4-12 **Cybersecurity Event Logs and Monitoring Management policy** to ensure that cybersecurity event records are collected, analyzed, monitored in time to proactively detect cyberattacks, and effectively manage their risks to prevent or reduce potential negative impacts on the university's business.

4-13 **Updates and Repair Packages Management Policy** to ensure that cybersecurity requirements are based on best practices and standards for updating and fixing packages of the university's systems, applications, databases, network devices, and information processing devices.

4-14 **Third-Party and Cloud Computing Cybersecurity Policy** to ensure that the university assets are protected from third-party cybersecurity risks (including Outsourcing and Managed Services) in accordance with the University's regulatory policies and procedures and related legislative and regulatory requirements.

4-15 **Penetration Testing Policy** to evaluate the effectiveness of cybersecurity enhancement and testing capabilities at the university by simulating actual cyberattack techniques and methods. This is performed when detecting unknown security vulnerabilities, which may lead to cyber-penetration of King Faisal University in accordance with relevant legislative and regulatory requirements.

4-16 **Vulnerabilities Management Policy** to ensure that technical vulnerabilities are detected and addressed in time in order to prevent and

reduce the potential exploitation by cyberattacks, and to reduce the effects on the university's work.

4-17 **Cybersecurity Incident and Threat Management Policy** to ensure that cybersecurity incidents are detected, identified on time, and effectively managed. This policy also ensure that cybersecurity threats are proactively dealt with to prevent or reduce potential negative impacts on the university's work, taking into account the decision no.37140, dated in 14/8/1438H.

4-18 **Database Security Policy** to ensure that the requirements of the cybersecurity infrastructure are based on the best practices and standards for protecting the university's databases to reduce cyber risks and protect those databases from internal and external threats.

4-19 **Web Application Security policy** to ensure that the university's internal and external web applications are protected from cyber risks.

4-20 **Industrial Control Systems Cybersecurity Policy** to ensure that cybersecurity is properly and effectively managed for protecting the availability, integrity, and confidentiality of the university assets and the Industrial Control Systems (OT\ICS) assets against cyber-attack (such as unauthorized access, sabotage, espionage, and manipulation) consistent with the university cybersecurity strategy. It also ensures cybersecurity risk management, relevant legislative and regulatory requirements, and other cybersecurity requirements adopted by the university.

4-21 **Cryptography Policy** to ensure the proper and effective use of encryption to protect the university's electronic information assets, following the university's policies and regulatory procedures and related legislative and regulatory requirements.

4-22 **Cybersecurity Risk Management Policy** to ensure that best practices and standards are defined for managing cybersecurity risks at the university, taking into account the confidentiality, availability, and integrity of information and technology assets.

4-23 **Cloud Computing and Hosting Cybersecurity Policy** to ensure that cyber risks are addressed and cyber security requirements for cloud computing and hosting are implemented appropriately and effectively, following the university's organizational policies and procedures, legislative and regulatory requirements, and relevant orders and decisions. It also

ensures the protection of the university's information and technology assets on cloud computing services, which are hosted or managed by third parties.

4-24 **Backup and Recovery Management Policy** to ensure the protection of the data, information, and technical settings systems and applications at the university from cyber-risk damage based on the university's regulatory policies and procedures, and related legislative and regulatory requirements.

4-25 **Data and Information Protection and Classification Policy** to ensure the protection of confidentiality, integrity, accuracy, and availability of university data and information, in accordance with the University's regulatory policies and procedures and related legislative and regulatory requirements.

4-26 **Physical and Environmental Security Policy** ensure that the university's information and technical assets are protected from unauthorized physical access, loss, stealing, and damage.

4-27 **Asset Management Policy** ensures that King Faisal University has an accurate and up-to-date inventory of assets that includes relevant details of all information and technological assets available at the university. This will help the university supports the operational processes and cybersecurity requirements and achieve the confidentiality, integrity, accuracy, and availability of information and technology assets.

5- Roles and Responsibilities

This section identifies, supports, and strengthens the responsibilities of implementing cybersecurity programs and requirements at King Faisal University. All parties involved in implementing cybersecurity programs and requirements must understand their roles and cybersecurity responsibilities at the university. This section also ensures that all parties involved in the application of cybersecurity controls at the university are aware of their responsibilities in implementing cybersecurity programs and requirements in the university. It also ensures compliance with cybersecurity requirements and related legislative and regulatory requirements which is considered a legislative requirement in items No. 1.4.1 and No. 1.9.1 of the Basic Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority.

1- The following list represents the most prominent roles and responsibilities necessary to approve cybersecurity policies and procedures, standards, and programs and implement and follow them. The cybersecurity unit represented by the Unit's CEO and Manager is to do the following work:

1-1-1 Writing to his Excellency the President of the University asking to form a committee for cybersecurity at the university, with the CEO of the Cybersecurity Unit being a member of that committee.

1-1-2 Writing to his Excellency the President of the University asking to approve the cybersecurity policies, and ensuring that the parties concerned are informed about the policy and applied, reviewed and updated it periodically.

1-1-3 The authorized party/parties responsible for human resources at the university, which employ(s) contracted employees through operational projects to apply the cybersecurity requirements related to university employees.

1-1-4 Coordinating with the university's legal affairs to ensure that the terms and requirements of cybersecurity and the maintenance of confidentiality of information (Non-disclosure Clauses) are legally binding on the contracts of university staff and third parties.

1-1-5 Coordinating with the Development, Quality and Relevant Sections of the IT Deanship to review and scrutinize cybersecurity controls in accordance with acceptable general auditing standards, and relevant legislative and regulatory requirements.

1-1-6 Coordinating with all university bodies in order to support cybersecurity policies, procedures, standards and programs, and provide all the resources required to achieve the objectives of King Faisal University, as well as educate and inform the university staff of the requirements of cybersecurity at the university and the importance of adhering to abide by them.

6- Adherence to the Polities

- The CEO of the Cybersecurity Unit, with the consent of His Excellency the President of the university, must periodically ensure that all university parties are committed to implementing and applying cybersecurity policies and their standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity policy may subject the violator to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

7- Exceptions

It is prohibited to bypass cybersecurity policies and standards without prior official authorization from the CEO of the Cybersecurity Unit, or the University's Cybersecurity Committee unless it conflicts with relevant legislative and regulatory requirements.

1. Cybersecurity Regulatory Compliance Policy

Objectives

The purpose of this policy is to provide best practice and standards-based cybersecurity requirements to ensure that the university's cybersecurity policy and regulations comply with the relevant legislative and regulatory requirements.

This policy aims to comply with the requirements of cybersecurity and related legislative and regulatory requirements, which is a legislative requirement in item 1.7.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cybersecurity Authority. For more details, please see Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all regulations and procedures of King Faisal University and is applied to all university employees.

Policy Items

1- The list of cybersecurity legislation and regulations and related requirements must be identified, documented and updated periodically.

2- Necessary Technologies must be provided to verify compliance with legislative and regulatory requirements related to cybersecurity.

3- Cybersecurity policies and procedures must be reviewed periodically to ensure that they comply with relevant legislative and regulatory requirements.

4- Ensuring that cybersecurity, policies and procedures are applied periodically.

5- Ensuring that relevant legislative and regulatory requirements are adhered to periodically by using appropriate tools such as:

- 5-1 Cybersecurity risk assessment activities.
- 5-2 Vulnerability management activities.
- 5-3 Penetration testing activities.
- 5-4 Security review of the source code.
- 5-5 Reviewing cybersecurity standards.
- 5-6 User questionnaires.
- 5-7 Interviews with stakeholders.
- 5-8 Reviewing permissions on the system and network.

5-9 Reviewing cybersecurity records and incidents.

6- The necessary batching actions must be defined and applied to batch vulnerabilities for all compliance requirements by stakeholders.

7- The Performance Measurement Index (KPI) should be used to ensure continuous development towards the adherence to applying cybersecurity controls and standards.

8- Appropriate procedures must be implemented to ensure compliance with legislative and regulatory requirements relating to intellectual property rights and software use.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity Unit.
- **Policy implementation:** Cybersecurity Unit.

Adherence to the Policies

- The CEO of the Cybersecurity Unit, with the consent of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying cybersecurity policies and standards.
- All university staff must adhere to this policy.
- Any violation of this policy and other policies related to cybersecurity may subject the violator to a regular procedure following the regular procedures of the university and or following the regular procedures issued by the relevant authorities.

2. Configuration and Hardening Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards relating to the protection, secure and control of the settings of data and technical assets and applications of King Faisal University to resist cyberattacks by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with the requirements of cybersecurity and related legislative and regulatory requirements, which is a legislative requirement in item 1.6.2.2 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cybersecurity Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all information and technical assets and applications of King Faisal University and is applied to all university employees.

Policy items

1- All information and technical assets used within the university as well as the approved applications and software must be defined and apply technical security standards on them.

2- Security technical standards for all authorized information and technical assets, applications, and software used inside the university must be developed, documented, and approved.

3- The settings of computers, systems, applications, network devices, and the university's security devices must be secured and set up in accordance with the technical security standards adopted to resist cyberattacks.

4- One of the following methods should be used to develop the technical security standards:

4-1 The supplier's Security Configuration Guidance in accordance with the university's regulatory policies and procedures, relevant legislative and regulatory requirements and international best practices.

4-2 The Security Configuration Guidance is from reliable and factory-compliant sources, such as the Center of Internet Security (CIS), the institute of Security and Networks and Systems Management (SANS), the National Institute of Standards and Technology (NIST), the Defense Information Systems Agency (DISA), the Security Technical Implementation Manual (STIG), etc.

4-3 Development of the technical security standards for the university in accordance with the nature of the business and the supplier's preparation and security manual and factory standards.

5- Controls for technical security standards should cover at least the following:

5-1 Breaking down or changing the factory and default accounts.

5-2 Preventing unwanted software installation.

5-3 Disabling unused network ports.

5-4 Disabling unused services.

5-5 Restricting the use of storage media and the external storage media.

5-6 Changing the default settings that may be exploited in cyberattacks.

6- The settings and security must be reviewed and applied in the following cases:

6-1 Reviewing the settings and security of the information and technical assets and applications periodically and ensuring that they are applied in accordance with approved security technical standards.

6-2 Reviewing the settings and security before launching projects and changes related to information and technical assets.

6-3 Reviewing the settings and security before launching applications.

6-4 Reviewing the settings and security of industrial control systems periodically and ensuring that they are applied in accordance with approved security technical standards.

6-5 Before making changes, the impact of change on all aspects of cybersecurity must be examined, and the cybersecurity unit must also be notified before implementing or making any change.

7- An Image must be adopted to prepare and secure the university's information and technical assets in accordance with security technical standards, and it must be kept in a safe place.

8- An approved Image must be used to install or update information and technical assets.

9- Required Technologies must be provided to manage settings and security and ensure that the settings can be applied or updated automatically for all information and technical assets on specific and planned times.

10- Security Content Automation Protocol (SCAP) settings must be provided to ensure that the settings are fully compliant with approved and applicable technical security standards, and any unauthorized changes must be reported.

11- The Key Performance Indictor (KPI) should be used to ensure continuous development of settings management and security.

12- Cybersecurity requirements for settings and security of the university's information and technical assets and applications should be reviewed annually or whenever there are changes in the legislative, regulatory or related standards.

13- Including cybersecurity risks in the Acceptable Use Policy.

14- When finalizing contracts, companies with certificates that demonstrate compliance with their cybersecurity standards, national cybersecurity standards, controls and policies must be given priority.

Roles and Responsibilities

Sponsor and owner of the policy document: CEO of the Cybersecurity Unit.

- **Policy Review and Update:** Cybersecurity unit.
- **Policy Implementation and Application:** Cybersecurity Unit.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with an agreement of his Excellency the President, must periodically ensure that all university affiliates are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subjected to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

3. Malware Protection Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards related to protecting users' devices, mobile devices and servers of King Faisal University from malware threats and reducing cyber risks resulting from internal and external threats by focusing on the basic objectives of protection, namely, confidentiality, integrity and availability of information.

This policy aims to comply with cybersecurity requirements and related legislative and regulatory requirements, which is a legislative requirement in item 2.3.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all users' devices and servers of King Faisal University and is applied to all university employees.

Policy Items

1- **General Items**

1-1 Cybersecurity Unit must identify and provide modern and advanced protection techniques and mechanisms and ensure their reliability.

1-2 Protection technologies and mechanisms must be applied to protect and securely manage users' devices, mobile devices and servers from malware.

1-3 Protection techniques and mechanisms must detect and remove all types of known malware, such as viruses, Trojan, Worms, Spyware, Adware, Root Kits.

1-4 Before selecting protection technologies and mechanisms, they must be ensured to be suitable for university operating systems such as Windows, UNIX, Linux, Mac, etc.

1-5 If updating protection technologies damages systems or business requirements, the protection techniques must be retrievable and backed up to the previous version.

1-6 Permissions to disable or cancel installation, or make changes to the settings of malware protection techniques must be restricted and given only to security system administrators.

2- Settings of Malware Protection Techniques and Mechanisms

2-1 The settings and mechanisms of protection techniques must be adjusted in accordance with the university's security technical standards, taking into account the supplier's guidelines and recommendations.

2-2 Antivirus settings must be adjusted on email servers to check all incoming and outgoing emails.

2-3 People belonging to the third parties are not allowed to connect to the university's network or wireless network without updating the antivirus software and adjusting the appropriate settings.

2-4 Malware protection software servers must be guaranteed, and the backup environment must be suitable for malware protection servers for tasks and inconsequent businesses.

2-5 Access to websites and other online sources known to host malware should be blocked using the Web Content Filtering mechanism.

2-6 Clock Synchronization must be applied centrally and from a precise and reliable source of all malware protection techniques and mechanisms.

2-7 Settings for malware protection techniques must be adjusted to verify suspicious content in isolated sources such as sandbox.

2-8 Periodic scans of users' devices and servers must be performed and their malware safety must be ensured.

2-9 Malware protection technologies should be automatically updated when new versions of the resource are available, taking into account the updates and repair management policy.

2-10 E-mail and web browsing technologies must be provided from Advanced Persistent Threats (APT Protection), which usually uses zero-day malware, and its safe application and management.

2-11 The settings of protection technologies must be adjusted by allowing only a specific list of Whitelisting files for applications and programs to work on servers for sensitive systems. (CSCC-2-3-1-1)

2-12 Servers for sensitive systems must be protected by end-point Protection technologies (CSCC-2-3-1-2).

2-13 Malware protection techniques must be managed centrally and they must be constantly monitored.

2-14 The Cybersecurity Unit must prepare periodic reports on the status of malware protection indicating the number and status of the devices and servers associated with protection technologies (e.g. updated, inundated, offline, etc.), and submit them to the CEO of the Cybersecurity Unit.

3- **Other Requirements**

3-1 The Cybersecurity Unit must ensure that all employees have the security awareness to deal with malware and reduce its risks.

3-2 The Key Performance Indicator (KPI) should be used to ensure continuous development to protect users' devices and servers from malware.

3-3 Cybersecurity requirements to protect the university's user devices and servers should be reviewed periodically.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation and implementation:** Cybersecurity Unit.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with an agreement of his Excellency the President, must periodically ensure that all university affiliates are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subjected to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

4. Server Security Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and servers standards for King Faisal University to reduce and protect cyber risks from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with cybersecurity requirements and related legislative and regulatory requirements, which is a legislative requirement in the item 2.3.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all servers of King Faisal University and is applied to all university employees.

Policy items

1- **General items**

1-1 All university servers must be selected and documented, and it must ensure that software is up-to-date and certified.

1-2 Technical Security Standards for servers used within the university must be developed and applied using the best international standards.

1-3 Server settings must be adjusted to the approved technical security standards before running the servers in the production environment.

1-4 All servers must be protected to control related cybersecurity risks.

1-5 Servers must be regularly backed up in accordance with the university's backup management policy to ensure that they can be restored during the accidental damage or accident. Daily backups of sensitive systems are needed.

1-6 Servers' software, including operating systems and application software should be updated and with the latest updates and security repair packages in accordance with the university's approved updates and repair management policy.

2- **Server Settings**

2-1 Image of the settings and security must be adopted for the university's server operating systems, and it must be kept in a safe place.

2-2 A supported image must be used to install or update server operating systems.

2-3 Server settings and security must be adopted, reviewed and updated periodically (at least every six months for sensitive system servers) (CSCC-2-3-1-6).

3- Access and Management

3-1 Access to the university's servers should be restricted to the authorized users and when needed.

3-2 Access to servers must be restricted and limited to the accounts of system supervisors. Reviewing the accounts and permission must be done periodically.

3-3 Access to servers for sensitive systems must be restricted and limited to the technical team members who have important permissions through Workstations. These devices must be isolated in a private system management network and prevented from being connected to any other network or service (e.g. e-mail service and the Internet).

3-4 Multi-Factor Authentication must be used to access servers for sensitive systems (CSCC-3-1-2-2).

3-5 Factory and default accounts must be stopped or changed. The unused services and network ports not used in operating system must be stopped, too.

3-6 Data stored on servers must be protected and encrypted in accordance with encryption controls and with relevant legislative and regulatory requirements. (ECC-2-8-3-3).

4- Servers Protection

4-1 Non-updated or unreliable servers should be prevented from connecting to the university network and placed in an isolated network to perform update in order to reduce related cyber risks that may lead to unauthorized access, malware, or data leaks.

4-2 Modern and advanced protection technologies and mechanisms must be used to protect against viruses, suspicious programs, activities and malware.

4-3 Only a specific list of Whitelisting files for applications and software should be allowed on the servers of the sensitive systems (CSCC-2-3-1-1).

4-4 The use of external storage media on servers must be restricted, and prior permission must be obtained from the cybersecurity unit before being used, and ensure that it is used securely.

4-5 Servers must be installed in the appropriate area of the network chart/structure according to their operational and legislative requirements to ensure that they are managed and that the necessary protection is applied to them effectively.

5- Operational Requirements for Servers Management

5-1 Servers must be managed centrally at the university to detect risks faster, and facilitate server management such as restricting access, installing updates packages, etc.

5-2 Servers operating in the Virtual Environment must be protected and managed securely depending on the risk assessment.

5-3 Server settings must be adjusted and event records sent to the Records and Monitoring System (SIEM) must be activated in accordance with the Event Records Management and Cybersecurity Monitoring Policy.

5-4 The Clock Synchronization of all servers must be performed centrally from a precise, reliable and certified source.

5-5 Requirements for operating servers must be provided securely and appropriately, such as providing a suitable and secure environment and restricting physical access to the server for the authorized personnel.

5-6 The IT Networks and Operating Systems Department should monitor the components of operational servers, ensure their effectiveness, availability, provide appropriate storage capacity, etc.

6- Vulnerability Management and Penetration Testing

6-1 Servers must be examined, vulnerability detected and processed based on the classification of detected weakness and cyber risks periodically and at least once a month for the sensitive system servers (CSCC-2-9-1-2).

6-2 Penetration tests on servers must be performed periodically and at least every three months on the sensitive system servers (CSCC-2-10-2).

6-3 Updates and security patch packages must be installed to address vulnerabilities and upgrade server efficiency and security, according to the updates and repairs management policy.

7- Servers Physical and Environmental Protection

7-1 Entry and exit from university facilities (e.g. doors and locks) must be identified and monitored.

7-2 Environmental factors such as heating, air conditioning, smoke, fire alarms and fire suppression systems should be identified and monitored.

7-3 Establishing appropriate physical security controls (e.g. surveillance cameras inside and outside the university data center, security guards, cable security, etc.) must be implemented.

8- **Other requirements**

8-1 The Key Performance Indicator (KPI) should be used to ensure continuous development of server protection.

8-2 Server management cybersecurity requirements should be reviewed at least annually or during the changes in legislative, regulatory or related standards.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** Cybersecurity Unit.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

5. Network Security Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards on network security for King Faisal University to reduce and protect cyber risks from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with the cybersecurity requirements and related legislative and regulatory requirements, a legislative requirement of the item 2.5.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all technical networks of King Faisal University and is applied to all university employees.

Policy items

1- **General items**

1-1 Identifying and documenting all network devices inside the university and making sure that all devices are updated and certified.

1-2 Documenting and adopting technical security standards for all network devices used inside the university.

1-3 Controlling the access to the university's networks in accordance with the access ID management policy and permissions, so that the network connection is available when needed and available only to the authorized users.

2- **Network access requirements**

2-1 Developing and adopting procedures for granting and eliminating access to the network in accordance with the university's access ID management policy and permission.

2-2 To gain access to the network, the user must apply to the IT deanship explaining the type, validity and justifications of the request.

2-3 In case of adding or modifying the firewall lists, the network administrator must document the business requirements and request information on the firewall system.

2-4 The username and password must be used to access the university's network in accordance with the access ID management policy and permissions.

2-5 Reviewing the Firewall Rules and settings periodically and at least every six months for the sensitive systems. (CSCC-2-4-1-2)

2-6 Providing the necessary protection when browsing and connecting to the Internet and restricting access to suspicious websites, file sharing sites and remote access sites.

2-7 Not to connect the wireless network to the university's internal network except because of an integrated study of the risks involved, and dealing with them to ensure the protection of private technical assets, data confidentiality and safety, and the protection of systems and applications related to the university's systems.

2-8 Connecting the sensitive systems to the university's wireless network is prevented.

2-9 Technologies must be provided to place restrictions and manage network ports, protocols and services.

2-10 The direct connectivity of any device to the local network of sensitive systems before checking it and ensures that protection elements are available to the acceptable level of sensitive systems (CSCC-2-4-1-3) is prevented.

3- Third-party Access Requirements

3-1 Granting third-party access to the university network is subject to the cybersecurity requirements referred to in the third-party cybersecurity policy.

3-2 Using the secure encryption and authentication techniques to transfer data to and from third parties.

3-3 Setting a certain time limit for the third parties to access the university network.

3-4 Reviewing the users and third parties' permissions periodically in accordance with the university's cybersecurity policies.

4- Network Protection

4-1 Networks must be physically and logically isolated and divided using Firewall and Defense-in-Depth. (ECC-2-5-3-1)

4-2 Applying the logical isolation to the sensitive systems network (VLAN).

4-3 Applying the logical isolation between the production environment network, the test environment network, and other networks.

4-4 It is prevented to connect sensitive systems to the Internet if they provide an internal service to the university. There is no very necessary need to enter the service from outside King Faisal University (CSCC-2-4-1-6).

4-5 Applying the logical isolation to the Voice Over IP (VOIP) and the data network.

4-6 Restricting the use of physical network ports in all university facilities by using Port Security or Port-Based Authentication to protect the network from the possibility of connecting unauthorized or suspicious devices.

4-7 Providing the protection systems to the Internet browsing channel to protect against and manage advanced continuous threats (APT Protection) that usually use viruses and pre-anticipated malware.

4-8 Blocking the direct connection to the internet internal network. The connection is made through the Internet Communications Distributor (Proxy) to analyze and filter data transmitted to and from the university network.

4-9 Adjusting firewall menu settings so that all types of connections between network parts are automatically blocked (Explicitly), and firewall lists are made available at the user's request and business requirements.

4-10 Necessary technologies must be provided for DNS security.

4-11 Advanced Intrusion Prevention Systems must be provided on all parts of the network and updated periodically.

4-12 Network APT systems must be provided on the sensitive systems network.

4-13 Internet browsing channel protection mechanisms from persistent advanced threats (APT) and previously unknown malware must be applied and managed. (ECC-2-5-3-8)

4-14 Distributed Denial of Service Attack (DDoS) systems must be provided on the sensitive external systems. (CSCC-2-4-1-8)

5- Physical and Environmental Security

5-1 Network devices must be kept in a safe and convenient environment; ensuring temperature and humidity are adjusted; and ensuring the availability of the backup power sources such as Uninterruptible Power Supply (UPS).

5-2 Physical access to network devices should be restricted to the authorized personnel only to save devices and protect them from theft or damage.

5-3 Access logs must be saved, and areas of network devices for sensitive systems (CCTV) must be monitored and reviewed periodically.

6- **Other requirements**

6-1 The Key Performance Indicator (KPI) should be used to ensure the continuous development of network security.

6-2 Network security requirements must be reviewed at least annually, or in the case of changes in legislative, regulatory or related requirements.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** Cybersecurity Unit.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

6. E-mail Security Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards related to protecting King Faisal University's e-mail from cyber and internal and external threats, by focusing on the basic objectives of protection, namely, the confidentiality, integrity and availability of information.

This policy aims to comply with the requirements of cybersecurity and related legislative and regulatory requirements, which is a legislative requirement of the item 2.4.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all king Faisal University e-mail systems and is applied to all university employees.

Policy items

1- Modern technologies must be used to protect email, analyze and filtering emails and block suspicious messages, such as Spam Emails and Phishing Emails.

2- E-mail systems must use user identification numbers and passwords to ensure that different users' connection are isolated.

3- Necessary technologies must be used to encrypt e-mail containing classified information.

4- Multi-Factor Authentication must be applied for online access and access through the Webmail page.

5- Emails must be archived and backed up periodically.

6- The responsibility for emailing must be determined to the public and shared accounts (Generic Account).

7- Zero-Day Protection technologies must be provided on email servers and the messages must be checked before they reach the user's mailbox.

8- The university's email domain must be documented by using the necessary means, such as the Sender Policy Framework method, to prevent e-mail fraud (Email Spoofing). The incoming message DMARC verification domains must also be verified.

9- Access to emails should be limited to university students and employees.

10- Actions must be taken to prevent the use of university e-mail for non-business purposes.

11- System Administrator is prevented to access to an employee's email information without prior authorization.

12- The size of the outgoing and incoming email attachments and the capacity of the mailbox for each user must be specified.

13- Emails sent outside the university must be appended through a disclaimer.

14- Necessary techniques must be applied to protect the confidentiality, integrity, availability and preservation of e-mail messages, including the use of encryption and data leak prevention techniques.

15- The Key Performance Indicator (KPI) should be used to ensure the continuous development of the e-mail system.

16- The Open Mail Relay service must be disabled.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation :** Cybersecurity Unit.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

7. User, Portable and Personal Devices Security Policy

Objectives

This policy aims to identify best practice and standards-based cybersecurity requirements to reduce cyber risks from the use of user devices (Workstations), Mobile Devices and Bring Your Own Device (BYOD) within King Faisal University, and to protect them from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy follows national legislative and regulatory requirements and relevant international best practices, a legislative requirement as mentioned in the items 2.3.1 and 2.6.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope of work and applicability

This policy covers all user devices, mobile devices and personal devices of employees within King Faisal University, and is applied to all university staff.

Policy items

General items

1-1 Data and information stored in users' devices, mobile devices and personal devices (BYOD) must be protected by classification using appropriate security controls to restrict access to this information, and prevent unauthorized workers from accessing it.

1-2 User hardware and mobile device software, including operating systems, software, and applications, must be updated. They must be provided with the latest updates and repair packages in accordance with the university's approved updates and repair management policy.

1-3 Configuration and Hardening controls for user and mobile devices must be applied in accordance with cybersecurity standards.

1-4 Employees should not be given important and sensitive permissions (Privileged Access) on users' devices and mobile devices, and the permissions must be granted in accordance with the principle of minimum powers and privileges.

1-5 Default user accounts must be deleted or renamed in the operating systems and applications.

1-6 Clock Synchronization must be applied centrally and from an accurate and reliable source for all user and mobile devices.

1-7 Users' and mobile devices must be provided with a text message (Banner) to allow authorized use.

1-8 A list of applications (Application Whitelisting) is allowed, and the data leakage and use of data monitoring systems, etc., are prevented.

1-9 Storage media for users' devices and mobile devices that are important and sensitive and have advanced powers must be encrypted in accordance with the university's encryption standard.

1-10 The use of external storage media must be prohibited , and prior permission must be obtained from the Cybersecurity Unit to have the power to use external storage media.

1-11 Users' devices, mobile devices and personal devices (BYOD) with unupdated or expired software (including operating systems, software, and applications) should not be allowed to connect to the university network to prevent security threats arising from expired software that is not protected by updates and repairs packages.

1-12 Users' devices, mobile devices and personal devices (BYOD) that do not have the latest protection software should be prevented from connecting to the university network to avoid cyber risks leading to unauthorized access, malware entry or data leakage. Protection software includes mandatory programs, such as antivirus, malware, host-based firewall, and host-based Intrusion Detection/Prevention.

1-13 User device settings and unused mobile devices must be adjusted to display a password-protected stop screen if the Session Timeout device is not used for as little time as possible.

1-14 User and mobile devices must be managed centrally through the University Domain Active Directory server or a centralized management system.

1-15 User and mobile device settings must be adjusted sing appropriate domain controllers to apply appropriate policies and install the necessary software settings.

1-16 Appropriate Group Policy must be implemented at the university and applied to all user and mobile devices to ensure that the university complies security regulations.

1- **User Device Security Cybersecurity Requirements**

2-1 User devices must be specified to the technical team who have important powers, isolated in a private system management network and not connected to any other network or service.

2-2 The settings of important and sensitive user devices which have advanced permissions to send records to a centralized recording and monitoring system must be adjusted in accordance with the event records management and cybersecurity control policy, while not being stopped by the user.

2-3 Users' devices must be physically secured within the university buildings.

2- **Portable Devices Security Cybersecurity Requirements**

3-1 Mobile devices must be denied access to sensitive systems but for a limited time, after conducting a risk assessment and taking the necessary approvals from the Cybersecurity Unit. (CSCC-2-5-1-1)

3-2 Hard disks of portable devices that have access to sensitive systems must be fully encrypted (Full Disk Encryption). (CSCC-2-5-1-2)

3- **Personal Device Security Cybersecurity Requirements (BYOD)**

4-1 Mobile devices must be managed centrally using mobile device management (MDM).

4-2 Data and information from King Faisal University stored on the personal devices of employees (BYOD) must be separated and encrypted.

4- **Other Requirements**

5-1 Performing a periodical back up to the data stored on users' devices and portable devices, in accordance with the university's backup policy.

5-2 King Faisal University data stored on mobile and personal devices (BYOD) is deleted in the following cases:

- Loss or theft of the mobile device.
- End or terminate the functional relationship between the user and the university.

5-3 Security awareness of the employees about the mechanism of use and responsibilities towards the devices should be raised, in accordance with the university's acceptable use policy and conduct awareness sessions for users with important and sensitive powers.

5-4 The Key Performance Indicator (KPI) should be used to ensure continuous development to protect users' devices and mobile devices.

5-5 The security policy for users' devices, mobile devices and personal devices should be reviewed annually, and the changes must documented and approved.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** Cybersecurity Unit.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

8. Acceptable Use of Assets Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements to reduce cyber risks related to the use of King Faisal University systems and assets, to protect them from internal and external threats, and to take care of the basic objectives of protection, namely, to maintain the confidentiality, integrity and availability of information.

This policy aims to comply with the cybersecurity requirements and related legislative and regulatory requirements, which is a legislative requirement in item No. 2.1.3 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all information and technical assets of King Faisal University and is applied to all university employees.

Policy items

1- **General items**

1-1 Information must be dealt with according to the specified classification, and in accordance with the policy of protecting and classifying data and information in such a way as to ensure that the confidentiality, integrity and availability of information are protected.

1-2 Violation of the rights of any person, copyrighted company, patent, other intellectual property, or similar laws or regulations, including, but not limited to, the installation of unauthorized or illegal software is prohibited.

1-3 Printed documents on the shared printer should not be left unattended.

1-4 External storage media should be kept safe and in a proper place, taking into consideration the temperature level and other environmental conditions.

1-5 It is forbidden to use the password of other users, including the password of the user manager.

1-6 You must adhere to the clean and secure office policy and make sure that the desktop and the display screen are free of classified information.

1-7 It is forbidden to disclose any information about the university, including information about the systems and networks, to any external/internal unauthorized party.

1-8 It is forbidden to publish information about the university through the media and social networks without prior authorization.

1-9 It is forbidden to use the university's systems and assets for achieving personal benefit, or to achieve any purpose that is not related to the university's activity and work.

1-10 It is prohibited to connect the personal devices to the networks and systems of the university without prior authorization, and in accordance with the Mobile Security Policy (BYOD).

1-11 Any activities aimed at bypassing the university's protection systems, including antivirus software, firewall and malware, are prohibited without prior authorization.

1-12 The Cybersecurity Unit has the right to monitor and periodically review work-related systems, networks and personal accounts to ensure the compliance with cybersecurity policies and standards.

1-13 Unauthorized persons are prohibited from entering sensitive places without prior authorization.

1-14 The ID card must be put on in all university facilities.

1-15 The Cybersecurity Unit must be notified if there is loss, stealing, or leak of information.

2- Computer Protection

2-1 External storage media usage is prohibited without prior authorization from the Cybersecurity Unit.

2-2 Any activity that would affect the efficiency and integrity of systems and assets, including activities that enable the user to obtain higher powers and privileges, is prohibited without prior permission from the Cybersecurity Unit.

2-3 The device must be locked before leaving the office through locking the screen, or signing out, whether it's leaving for a short time or when working hours are over.

2-4 It is forbidden to leave any classified information in easily accessible places, or to be accessed by unauthorized persons.

2-5 It is forbidden to install external tools on the computer without prior permission from the IT deanship.

2-6 The Cybersecurity Unit should be notified when there is any suspicious activity that may cause damage to King Faisal University computers or assets.

3- **Acceptable Use of Internet and Software**

3-1 The cybersecurity unit should be informed about the suspicious sites that should be blocked.

3-2 It is must be ensured that the intellectual property rights are not violated while downloading information or documents for business purposes.

3-3 The use of unlicensed software or other intellectual property is prohibited.

3-4 A secure and authorized browser to access the internal network or the Internet must be used.

3-5 It is forbidden to use technologies that allow proxy or firewall.

3-6 It is forbidden to download software and tools or install them on university assets without prior permission from the IT deanship.

3-7 It is forbidden to use the Internet for non-business purposes including downloading media and files and using file-sharing software.

3-8 The cybersecurity unit should be notified when cybersecurity risks are suspected, and security messages that may appear while browsing the Internet or internal networks should be treated with caution.

3-9 A security test is prohibited for the purpose of detecting vulnerabilities, including hacking testing, or monitoring the university's network, systems, networks and third-party systems without prior authorization from the Cybersecurity Unit.

3-10 File-sharing sites are prohibited without prior authorization from the Cybersecurity Unit.

3-11 It is forbidden to visit suspicious sites including hack-learning sites.

4- **Acceptable Use of E-mail and Communications System**

4-1 It is forbidden to use e-mail, phone, fax, or e-fax for non-business purposes, in accordance with cybersecurity policies and standards.

4-2 It is forbidden to trade messages containing inappropriate or unacceptable content, including messages circulating with internal and external parties.

4-3 Encryption techniques should be used when sending sensitive information by email or communication systems.

4-4 The university's email address should not be registered at any location that has nothing to do with the work.

4-5 The Cybersecurity Unit must be notified when there are emails containing content that may cause damage to the university's systems or assets.

4-6 The University has the right to disclose the contents of emails after obtaining the necessary permits from the holder of the authority and the cybersecurity unit in accordance with the relevant procedures and regulations.

4-7 It is forbidden to open suspicious or unexpected emails and attachments even if they appear to be from reliable sources.

5- **Visual Meetings and Web-based Communications**

5-1 It is prohibited to use unauthorized tools or software to hold video meetings.

5-2 It is forbidden to make contacts or hold video meetings that are not related to work without prior authorization.

6- **Use passwords**

6-1 You must choose secure passwords for the university systems and assets. You should also choose different passwords from personal account passwords, such as personal mail accounts and social media sites.

6-1 It is forbidden to share your password through any means, including electronic correspondence, voice communications, and paper writing. All users should not disclose their passwords to any other party, including co-workers and IT deanship employees.

6-2 The password provided with the system administrator must be changed.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** the Cybersecurity Unit and all employees.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

9. Cybersecurity Review and Audit Policy

Objectives

This policy aims to identify cybersecurity requirements based on best practices and standards to review and scrutinize the cybersecurity controls of King Faisal University and to ensure that they are applied in accordance with the university's regulatory policies and procedures, relevant national legislative and regulatory requirements, and international requirements regulatory based on King Faisal University.

This policy follows national legislative and regulatory requirements and relevant international best practices, and is a legislative requirement as stated in the item 1.8.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all cybersecurity controls at King Faisal University and is applied to all university employees.

Policy items

1- **General items**

1-1 The Cybersecurity Unit should periodically monitor the application of cybersecurity controls, and review compliance with the National Cybersecurity Authority's Basic Cybersecurity Controls (ECC:1-2018) and Cybersecurity Controls for Sensitive Systems (CSCC-1:2019).

1-2 The application of cybersecurity controls must be reviewed and scrutinized periodically by parties independent of the cybersecurity unit, and third parties can be used with regular procedures in this regard.

1-3 The application of cybersecurity controls to sensitive systems must be reviewed at least once every three years by parties independent of the cybersecurity unit from inside the university.

1-4 It must be ensured that cybersecurity controls are applied periodically, at least once a year to sensitive systems to ensure that they are aligned with basic cybersecurity controls (ECC:1-2018) and cybersecurity controls for sensitive systems (CSCC-1:2019).

1-5 Cybersecurity audit procedures must be identified and documented.

1-6 The results of a cybersecurity review and audit should be documented and discussed with stakeholders.

1-7 The results should be presented to the university's cybersecurity committee and the authority, and they should include the scope of the review and audit, discovered observations, recommendations and corrective actions, risk assessment and the feedback-processing plan.

1-8 The following responsibilities table (RACI Chart) should be adopted in the implementation of cybersecurity audits and audits, in accordance with the table below (Table 1 - Distribution of Powers and Responsibilities matrix in the implementation of cybersecurity audits and audits).

	External Audit Party	Department of Development and Quality in general it	Cybersecurity Unit	CEO of the Cybersecurity Unit	Chairman of the University's Cybersecurity Committee
Cybersecurity Review	R	R	R	A	I
Cybersecurity Audit	R	R	I	I	A
Implementation of corrective measures	C / I	C / I	R	R	A

R: Responsible

A: Administrator

C: Consultant

I: Informed

2- **Other requirements**

2-1 The Cybersecurity Unit must take proactive and corrective action on the results of the audit.

2-2 The Cybersecurity Unit should identify and analyze the factors that led to these observations, find out their causes and reduce their co-occurrence.

2-3 The cybersecurity audit policy should be reviewed annually. It should be documented and approved.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.

- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** The Department of Development and Quality at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

10. Identity and Access Management Policy

Objective

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards relating to the management of access identities and permissions over king Faisal University's information and technical assets to reduce cyber risks and protect them from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with cybersecurity requirements and related legislative and regulatory requirements, a legislative requirement in the item 2.2.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope of and Applicability

This policy covers all information and technical assets of King Faisal University and is applied to all university employees.

Policy items

1- **Identity and Access Management**

1-1 **Access Management**

1-1-1 Documenting and approving an access management procedure that clarifies the mechanism for granting access to information and technical assets, modifying and deleting them at the university, monitoring this mechanism and ensuring its application.

1-1-2 Creating User Identities in accordance with the university's legislative and regulatory requirements.

1-1-3 Authentication of the user identity before giving the user access to information and technical assets.

1-1-4 Documenting and approving matrix to manage user identity and access based on access control principles and the following powers:

1-1-4-1 Need-to-Know and Need-to-Use principle.

1-1-4-2 Segregation of Duties principle.

1-1-4-3 Least Privilege principle.

1-1-5 Applying the verification and access controls to all technical and informatics assets at the university through an automated centralized access control system, such as lightweight Directory Access Protocol (LDAP).

1-1-6 Preventing the use of Generic User accounts to access the university's information and technical assets.

1-1-7 Adjusting system settings to be automatically closed after a specified period of time (Session Timeout) (recommended not to exceed 15 minutes).

1-1-8 Disabling unused user accounts within a specified period of time (it is recommended that the period should not exceed 90 days).

1-1-9 Adjusting the settings of all identity management and access systems to send records to a centralized recording and monitoring system in accordance with the event records management and cybersecurity control policy.

1-1-10 Users are not granted access or direct handling of databases of the sensitive systems except the database administrators. [CSCC-2-2-1-7]

1-1-11 Documenting and approving clear procedures to deal with Service Accounts and ensure that they are securely controlled for the applications and systems, and that interactive login is disabled through them. (CSCC-2-2-1-7)

1-2 Access Permission

1-2-1 User Account Access Requirements

1-2-1-1 Giving permission to access based on the user's request he/she applies to through a form or the system adopted by the direct manager and system owner specifying the name of the system, the type of application, validity and duration (if the access authority is temporary).

1-2-1-2 Giving the user access to the university's information and technical assets in accordance with their roles and responsibilities.

1-2-1-3 Following a unified mechanism for creating user identities in such a way that you can track activities performed using User ID and link them to the user, such as typing <the first letter of the first name> point < last name>, or writing the employee number already identified by the university's human resources authority/entities.

1-2-1-4 Disabling the user from performing multiple computers login at the same time (Concurrent Logins).

1-2-2 Access to Important and Critical Accounts Requirements

In addition to the controls mentioned in the User Account Access Requirements section, the controls described below should apply to accounts with important and sensitive permissions:

1-2-2-1 Assigning an individual user access for the users who request important and sensitive powers (Administrator Privilege) based on their duties, taking into account the principle of separation of tasks.

1-2-2-2 Password History must be activated to track the number of passwords that have been changed.

1-2-2-3 Changing the names of default accounts, especially accounts with important and sensitive powers such as Root, Admin, and Sys id.

1-2-2-4 Preventing the use of accounts with important and sensitive powers in day-to-day operations.

1-2-2-5 Examining the users accounts with important and sensitive powers over technical and information assets through the Multi-Factor Authentication Mechanism (MFA) using at least two of the following methods:

- Knowledge (something the user knows "like a password").
- Possession (something that the user only owns "such as a program or random number generating device or temporary SMS to sign in," called "One-Time-Password").
- Feature (a characteristic or vital feature related to the user himself only "e.g. fingerprint").

1-2-2-6 Access and follow-up to the sensitive systems and the systems used to manage and follow sensitive systems should require the use of multi-element identity verification (MFA) for all users.

1-2-3 Remote access to the university network

1-2-3-1 Grant remote access to information and technical assets after prior authorization from the Cybersecurity Unit and restrict access using Multi-Factor Authentication (MFA).

1-2-3-2 Saving the observation event records of all private remote access sessions according to the sensitivity of information and technical assets.

1-3 Access Cancel and Change

1-3-1 The authority/entities responsible for human resources at the university must notify the IT deanship to take the necessary action when the user changes his or her duties, or terminates his or her work from King Faisal University. The IT deanship suspends or modifies the user's access permission based on their new functions.

1-3-2 If the user's permissions are stopped, the user's event records are prevented from being deleted and saved in accordance with the Event Records Management and Cybersecurity Monitoring Policy.

2- Identity and Access Review

2-1 Reviewing the user IDs, verifying the access to information and technical assets in accordance with the user's functional functions based on periodic access control principles and powers, and reviewing access identities on the sensitive systems at least once every three months.

2-2 Reviewing User Profile of information and technical assets based on the entry control principles and permissions periodically, and reviewing the access of the sensitive systems at least once a year.

2-3 All failed and successful access attempts must be recorded and documented periodically.

3- Password Management

3-1 Applying a secure high-standard password policy for all accounts inside the university. The table below (table 2 - password controls) includes examples of password controls for each user:

Password Controls	All Users	Privileged Users	Service accounts
Minimum number of password characters	8 characters, numbers or symbols	12 characters, numbers or symbols	8 characters, numbers or symbols
Password record	Remember 5 passwords	Remember 5 passwords	Remember 5 passwords
Maximum password duration	6 months	45 days	45 days
Password Complexity	Active	Active	Active
An example of password complexity	D_dyW5$_	R@rS%7qY#b!u	r? M4d5V=
Account closing time	30 minutes or until the system opens	30 minutes or until the system opens	30 minutes or until the system opens
Account closing limit	5 incorrect attempts to log in	5 incorrect attempts to login	There are no attempts.
Resetting the account closing counter after a certain period of time	30 minutes (manager manually opens the closed account)	30 minutes (manager manually opens the closed account)	Not found
Using MFA	Activated to remote access only	Active	Not Active

3-2 Password Standards

3-2-1 The password (8) must include at least 8 characters.

3-2-2 The password must be complex and include at least three of the following characters:

3-2-2-1 Upper Case Letters.

3-2-2-2 Small letters (Lower Case Letters).

3-2-2-3 Numbers (1235).

3-2-2-4 Special character (#%*@).

3-2-3 Users must be notified before the password expires to change the password.

3-2-4 Settings of all information and technical assets, when requesting a temporary password change, must be adjusted when the user logs in for the first time.

3-2-5 All default passwords must be changed for all information and technical assets before they are installed in the production environment.

3-2-6 Default Community String passwords (e.g. Public, Private and System) and the Simple Network Management Protocol (SNMP) must be changed. The must also be different from the passwords used to log into the technical assets involved.

3-3 Password Protection

3-3-1 All passwords for the university's information and technical assets must be encrypted in a format that is not readable as they are entered, transferred and stored in accordance with the encryption policy.

3-3-2 The password must be masked when you enter it on the screen.

3-3-3 Remember Password must be disabled on the university's systems and applications.

3-3-4 Preventing the use of known words (Dictionary).

3-3-5 The user's password must be submitted safely and reliably.

3-3-6 If the user requests a reset of the password by phone, internet or any other means, the user's identity must be verified before the password is reset.

3-3-7 Passwords for service accounts and accounts with important and sensitive access must be protected and stored securely in an appropriate place (inside a closed and sealed envelope), or use privilege Access Management Solution techniques.

4- **Other Requirements**

4-1 The Key Performance Indicator (KPI) should be used to ensure the continuous development of access identities and powers management.

4-2 Reviewing the application of cybersecurity requirements to manage identities and access periodically.

4-3 This policy must be reviewed at least annually, or when there are changes in legislative, regulatory or related requirements.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** Related departments at the Deanship of Information Technology, the university's human resources officers, and the Cybersecurity Unit.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

11. Human Resources Cybersecurity Policy

Objectives

The purpose of this policy is to provide best practice-based cybersecurity requirements to ensure that cybersecurity risks and requirements for employees (employees and contractors) at King Faisal University are effectively addressed before, during and when their work is completed/terminated.

This policy aims to comply with the requirements of cybersecurity and related legislative and regulatory requirements, which is a legislative requirement in the item 1.9.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all regulations of King Faisal University and is applied to all university employees.

Policy items

General items

1-1 Cybersecurity requirements for employees must be determined.

1-2 Positions related to sensitive systems at the university must be occupied by competent citizens.

1-3 Human resources cybersecurity controls must be implemented during the university's lifecycle, which includes the following stages:

- Before hiring
- During the working period
- When the working period ends

1-4 University employees must understand and approve their functional roles, cybersecurity-related conditions and responsibilities.

1-5 Cybersecurity responsibilities and non-disclosure agreement clauses must be included in the university employees' contracts (to include during and after the termination of the career at King Faisal University).

1-6 Cybersecurity-related violations must be included in the list of human resources violations at King Faisal University.

1-7 It is prohibited to review the employee information without prior authorization.

1-8 The Key Performance Indicator should be used to ensure the continuous development of human resources cybersecurity requirements.

Before Hiring

2-1 Employees must adhere to cybersecurity policies before being given access to university systems.

2-2 Employees' roles and responsibilities must be defined taking into account the application of the principle of non-conflict of interest.

2-3 Employees' roles and cybersecurity responsibilities must be defined in the job description.

2-4 Cybersecurity roles and responsibilities should include:

- Protecting all university assets from unauthorized access or damage.
- Implementing all required cybersecurity-related activities.
- Adhering to the university's cybersecurity policies and standards.

2-5 Conducting a security survey on the cybersecurity personnel, technical functions with important and sensitive powers, and functions related to sensitive systems.

During Work

3-1 Raising the awareness of cybersecurity among university employees, including cybersecurity policies and standards periodically.

3-2 The human resources authority/parties at the university must inform the deanship of Information technology and relevant departments of any change in the roles or responsibilities of the employees, in order to take the necessary actions to revoke or modify access permissions.

3-3 Ensuring that human resources cybersecurity requirements are met.

3-4 Compliance with cybersecurity should be included in aspects of employee evaluation.

3-5 Ensuring that the Need-to-know principle is applied in task assignment.

Work Termination

4-1 Professional termination procedures must be defined to cover cybersecurity requirements.

4-2 The human resources officers at the university must inform the relevant units with the work end or termination to take the appropriate action.

4-3 Ensuring that all university assets are returned and that the entry permissions of employees on their last working day are revoked before they receive the necessary clearances.

4-4 Responsibilities and duties that will remain after the end of the service of university employees, including the Agreement on the Confidentiality of Information, must be determined, if those responsibilities and duties are included in all employee contracts.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** the body/entities responsible for human resources at the university.

Adherence to the Policy

The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.

All university employees must adhere to this policy.

Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

12. Event Log Management and Cybersecurity Monitoring Policy

Objectives

The purpose of this policy is to provide best practice and standards-based cybersecurity requirements to reduce cyber risks, and to protect King Faisal University's information assets from internal and external threats, using event log management and cybersecurity observation.

This policy aims to comply with the requirements of cybersecurity and the relevant legislative and regulatory requirements, which is a legislative requirement in item No. 2.12.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all juvenile record management systems, and the cybersecurity surveillance of King Faisal University, and is applied to all university employees.

Policy items

1- **General items**

1-1 Security Information and Event Management (SIEM) must be provided to collect records of cyber events of information assets, systems, applications, databases, networks and protection systems at the university. These records must minimally contain the following:

1-1-1 Event Type
1-1-2 Location of Event or System
1-1-3 Date and Time of Event
1-1-4 User or Tool
1-1-5 Success vs. Failure

2- **Events to be Recorded**

2-1 Systems to monitor must do event records when an event occurs, at least the following:

2-1-1 Event Logs related to cybersecurity on all technical components of sensitive systems (operating systems, databases, storage, applications, and networks).

2-1-2 Event Logs related to cybersecurity for the industrial network and related communications.

2-1-3 Events of accounts with important and sensitive permissions over information assets.

2-1-4 Browsing, Internet, and wireless events.

2-1-5 Information transferring through external storage media.

2-1-6 Making illegal changes to records, and sensitive system files through File Integrity Management (FIM) techniques.

2-1-7 Changing system, network, or service settings, including downloading updates, fixes, or other changes to installed software.

2-1-8 Suspicious activities, such as activities detected by the Intrusion Prevention System (IPS)

2-5 Security procedures and standards that apply best practices for keeping event records must be set in a way that ensures their security from modification, deletion, or unauthorized access.

2-5 Event records must be monitored and analyzed periodically by classification, including monitoring and analyzing the behavior of the user of sensitive systems.

2-5 Clock Synchronization must be performed centrally, using a precise and reliable source, for all monitored systems.

2-5 The Key Performance Indicator (KPI) should be used to ensure the continuous development of the event log management and cybersecurity monitoring system.

2-6 The event records must be archived and backed up periodically.

2-7 The duration of keeping records of cyber events must be at least 12 months, and 18 months for sensitive systems, in accordance with domestic policies and relevant legislative and regulatory requirements.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** Cybersecurity Unit.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.

- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

13. Updates and Repair Package Management Policy

Objectives

This policy aims to identify cybersecurity requirements based on best practices and standards related to the management of updates and repair packages for systems, applications, databases, network devices and information processing devices of King Faisal University. It aims at reducing cyber risks and protect them from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy follows national legislative and regulatory requirements and relevant international best practices, which is a legislative requirement as stated in the item No. 2.3.3.3 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all systems, applications, databases, network devices, information-processing devices, and industrial control devices and systems of King Faisal University, and is applied to all university employees.

Policy items

1- Controlling the Patch Management to ensure that systems, applications, databases, network devices, and information processing devices are protected.

2- Downloading updates and repair packages from licensed and reliable sources in accordance with the procedures followed inside the university.

3- Utilizing reliable and secure technical systems to conduct a periodic scan to detect vulnerabilities and package updates, and following their implementation.

4- IT-related sections must examine the updates and repair packages in the Test Environment before installing them on systems, applications, and processing devices in the production environment to ensure that updates and repair packages are compatible with the systems and applications.

5- Rollback Plan should be prepared, developed and implemented if updates and repair packages adversely affect the performance of systems, applications, or services.

6- The cybersecurity committee at the university should make sure that updates and repair packages are applied periodically.

7- Priority should be given to updates and repair packages that address vulnerabilities depending on the level of the risk associated.

8- Scheduling updates and repairs following the stages of software versions that the vendor offers.

9- Installing updates and repairs at least once a month for sensitive internet-connected systems, and once every three months for internal sensitive systems. (CSCC-2-3-1-3).

10- Installing updates and repairs to the technical assets as described in the following table (table 3 - duration of the installation of updates and repairs):

Asset Type	Duration of Repetition to Install Updates	
	Information and technical assets	Information and technical assets of sensitive systems
Operating systems	Per month	Per month
Databases	Three months.	Per month
Network devices	Three months.	Per month
Applications	Three months.	Per month

11- The process of managing updates and repairs should follow the requirements of the change management process.

12- In the event of high-risk security vulnerabilities, emergency updates and repair packages must be installed in accordance with Emergency Change Management.

13- Updates and repairs must be downloaded to the Centralized Patch Management Server before installing them on the systems, applications, databases, network devices and information processing devices, excluding updates and repair packages that do not have supported automated tools.

14- After installing updates and repair packages, independent and reliable tools must be used to make sure that the issues are effectively addressed.

15- The Key Performance Indicator (KPI) should be used to ensure continuous development of the management of updates and repair packages.

16- Reviewing the policy of managing updates and repair packages and procedures annually, and documenting and approving changes.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** it deanship.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

14. Third-party Cybersecurity Policy

Objectives

This policy aims to identify cybersecurity requirements to ensure that king Faisal University's information and technical assets are protected from third-party cybersecurity risks, including IT support services and services managed in accordance with King Faisal University's regulatory policies and procedures.

This policy follows national legislative and regulatory requirements and relevant international best practices, and is a legislative requirement as mentioned in the item 4.1.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy is applied to all services provided by the external parties of King Faisal University as well as all university employees.

Policy Items

1- General Items

1-1 Unified procedures must be documented and approved to manage King Faisal University's relationship with external parties before, during and after the business contracts.

1-2 External frameworks provided for services must be carefully identified and selected in accordance with king Faisal University's regulatory policies and procedures, and related legislative and regulatory requirements.

1-3 A risk assessment of third parties and the services provided must be carried out by reviewing third-party projects inside the university and reviewing records of cyber events of third-party services (if possible) before and during the contract.

1-4 Contracts and agreements with third parties must be prepared to ensure that the external party is committed to applying the university's cybersecurity requirements and related legislative and regulatory requirements.

1-5 Contracts and agreements with third parties must be reviewed by the university's legal affairs authority to ensure that the terms of the agreement are binding and that their violation exposes the third party to legal accountability.

1-6 Contracts and agreements must include Non-Disclosure Clauses and secure deletion of the university data at the end of third party's service.

1-7 Cybersecurity requirements with third parties should be reviewed periodically.

1-8 Third party cybersecurity policy should be reviewed annually, and the changes must be documented and approved.

2- Cybersecurity Requirements for the Outsourcing or Managed Services Provided by the Third Parties

2-1 For outsourcing support services or managed services, the external party must be carefully selected, and the following must be verified:

2-1-1 Currying out a cybersecurity risk assessment and ensuring that those risks are controlled, before signing contracts and agreements or when changing relevant legislative and regulatory requirements.

2-1-2 Operations centers for managed and controlled cybersecurity services that use remote access must be entirely located within the Kingdom. (ECC-4-1-3-2)

2-1-3 Outsourcing services on sensitive systems must be through national companies and agencies, in accordance with the relevant legislative and regulatory requirements. (CSCC-4-1-1-2)

3- Cybersecurity Requirements for the Third-party Employees

3-1 Screening or Vetting must be conducted for outsourcing service companies, outsourcing service and managed services employees who works on the sensitive systems. (CSCC-4-1-1-1)

3-2 Cybersecurity responsibilities and non-disclosure Clauses must be included in third-party employee contracts (to include during and after the termination/end of the career relationship with the University).

4- Documentation and Access Controls

4-1 Third parties must develop and follow a carefully documented formal process to grant and eliminate access to all information and technical systems that process, transmit or store university information in line with the university's cybersecurity requirements and cybersecurity controls objectives.

4-2 There must be a way to access the university data and handle it in a secure and controlled manner.

4-3 Password controls must be applied to all users who have access to university information in line with the university's cybersecurity requirements and cybersecurity controls objectives.

4-4 A multi-Factor Authentication must apply to access to sensitive systems that process, transmit or store university information.

4-5 Access rights must be revoked as soon as the services of any employee who works for the third parties and has access to the university's information or information and technical assets or if his or her career is changed.

4-6 Third parties must review access rights periodically in accordance with the university's cybersecurity policies.

4-7 All auditing records must be stored, maintained and provided at the university's request.

5- Cybersecurity Requirement for Change Management

5-1 Third parties must follow the formal and appropriate change management process in accordance with the university's policies and procedures, and cybersecurity requirements.

5-2 The changes made to the university's information and technical assets must be reviewed and tested before being applied to the Production Environment.

5-3 The stakeholders at the university must be informed of the major planned changes as well as those changes made on the university's information and technical assets.

6- Requirements of the Cybersecurity Incident Management and Business Continuity

6-1 The terms of contracts and agreements with third parties must include requirements for reporting cybersecurity incidents and informing the university when a cybersecurity incident involving the third party.

6-2 In case of a cybersecurity incident, the third party must identify and document communication procedures between the third party and the university, and review and update these procedures periodically.

6-3 An appropriate business continuity plan should be developed to avoid the lack of services provided to the university in accordance with the requirements of the university's business continuity plan.

7- Requirements for Data and Information Protection

7-1 Third parties must process, store and destroy university data and information in accordance with the university's approved data and information protection policy.

7-2 Appropriate encryption controls must be applied to protect the university's data and information and ensure that it is kept confidential, safe and available in accordance with the university's encryption standard.

7-3 University data and information must be backed up periodically in accordance with the university's backup management policy.

7-4 Data and information of the university found in the sensitive systems and personal data (Data privacy), which are processed by the third parties , should not be processed, stored or used in the test environment except when strict controls have been used to protect such data as Data Masking techniques, Data Scrambling techniques, or Data Anonymization techniques. (CSCC-2-6-1-1)

7-5 Data and information of the university found in the sensitive systems, which are handled by third parties should not be transferred outside the production environment. (CSCC-2-6-1-5)

7-6 Data and information of the university found in the sensitive systems which are processed by third parties must be classified in accordance with the Data and Information Protection and Classification Policy (CSCC-2-6-1-2).

8- Auditing

8-1 The University must audit the relevant processes and regulations when necessary or appropriate.

8-2 All third-party facilities and employees must cooperate fully with the University's event log review and audit activities, including activities, which have been carried out.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy Update and Review:** Cybersecurity Unit.
- **Implementation of the policy:** Cybersecurity Unit and the departments related to the IT Deanship, the authority responsible for human resources at the university, the legal affairs authority at the university and the procurement and tenders authorities.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

15. Penetration Test Policy

Objectives

The purpose of this policy is to provide best practice-based cybersecurity requirements in assessing and testing the effectiveness of KFU's cybersecurity enhancement capabilities by simulating actual cyberattack techniques and methods, and to detect unknown security vulnerabilities that may lead to cyber-penetration by focusing on the basic protection objectives: Confidentiality, integrity and availability of information.

This policy aims to comply with the requirements of cybersecurity and related legislative and regulatory requirements, which is a legislative requirement in the item 2.11.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all sensitive systems and their technical components, and all services provided externally (via Internet) and their technical components, including infrastructure, websites, web applications, smartphone and tablet applications, e-mail and remote access at King Faisal University. It is applied to all university staff.

Policy Items

1- **General Requirements**

1-1 The university must conduct penetration tests periodically to assess and examine the effectiveness of cybersecurity enhancement capabilities.

1-2 The Cybersecurity Unit identifies the systems, services and technical components on which the penetration test must be conducted in accordance with the relevant legislative and regulatory requirements.

1-3 The university must conduct a penetration test on all externally provided services and technical components periodically. (ECC-2-11-3-1)

1-4 The penetration test must not affect the systems and services provided at the university.

1-5 The university must conduct a penetration test on sensitive systems and their technical components at least every six months. (CSCC-2-10-2)

1-6 A penetration test must be performed to detect all security vulnerabilities, including those usually caused by application development error, Configurations Faults and Exploitability of Identified Vulnerability.

1-7 Penetration testing procedures should be developed, approved and disseminated, taking into account their non-impact on the university's business.

1-8 The cybersecurity unit must identify or approve penetration testing methods, tools and techniques used by the internal or external penetration test team before the penetration test process begins.

1-9 If an external party is authorized to conduct the penetration test on behalf of the university, the application of all third-party cybersecurity requirements must be checked in accordance with the university's third-party cybersecurity policy.

1-10 The results of the penetration test should be classified based on their seriousness and addressed according to the cyber risks involved and in accordance with the university's risk management methodology.

1-11 An action plan should be developed to address the results of the penetration test in which the impact of the risks, the mechanism of their treatment, the person responsible for their application and the time required to implement them should be developed.

2- **Other Requirements**

2-1 The Key Performance Indicator (KPI) should be used to ensure the continuous development of the penetration testing processes.

2-2 The application of cybersecurity requirements for penetration tests at the university should be reviewed periodically. (ECC-2-11-4)

2-3 This policy should be reviewed at least once a year.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** the Cybersecurity Unit and the related department at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

16. Vulnerabilities Management Policy

Objectives

The purpose of this policy is to provide best practice and standards-based cybersecurity requirements to ensure that technical vulnerabilities are detected and effectively addressed to prevent or reduce the potential cyberattacks. These requirements minimize the implications of King Faisal University's work and protect it from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with the requirements of cybersecurity and related legislative and regulatory requirements, which is a legislative requirement in the item No. 2.10.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all information and technical assets at King Faisal University. It is applied to all university employees.

Policy Items

1- **General requirements**

1-1 The university should periodically examine vulnerabilities to detect and evaluate technical vulnerabilities and address them effectively.

1-2 The Cybersecurity Unit determines which systems, services and technical components to check the vulnerabilities in accordance with the relevant legislative and regulatory requirements.

1-3 The Cybersecurity Unit should make sure that reliable methods and tools are used to detect vulnerabilities.

1-4 Procedures for implementing the examination and discovery of vulnerabilities must be developed and approved in accordance with the relevant legislative and regulatory requirements.

1-5 If a third party is authorized to test and detect vulnerabilities on behalf of the university, all third-party cybersecurity requirements must checked and applied in accordance with the university's third-party cybersecurity policy.

2- **Vulnerabilities Assessment Requirements**

2-1 Vulnerabilities must be tested and detect before providing services or systems online or when making any change to the sensitive systems.

2-2 Vulnerabilities should be classified by their severity and addressed according to the cyber risks they entail in accordance with the university's risk management method.

2-3 The university must assess and address vulnerabilities for all technical assets periodically. (ECC-2-10-3-1)

2-4 The university must assess and address vulnerabilities in the technical components of internal sensitive systems at least every three months. (CSCC-2-9-1-3)

2-5 The university must assess vulnerabilities in the technical components of sensitive external and Internet-connected systems once a month. (CSCC-2-9-1-2)

3- **Vulnerabilities Processing Requirements**

3-1 Once the vulnerabilities have been assessed, a report about them should be prepared explaining their existence and classification, and the proposed recommendations for addressing them.

3-2 After sending the vulnerabilities assessment report to the responsible party and fixing them, the discovered vulnerabilities must be examined again to ensure that they are fixed.

3-3 Updates and Patches Packages should be adopted from reliable and secure sources and in accordance with the updates and repair packages policy.

3-4 Newly discovered Critical Vulnerabilities must be fixed following the university's change management mechanisms. (CSCC-2-9-1-3)

3-5 If the vulnerability cannot be fixed for any reason, it is necessary to apply other controls such as shutting down the security vulnerability service, providing an alternative protection Control (Compensating Control) such as access control through firewalls and other solutions, monitoring the vulnerability of actual attacks, and informing the incident response team of this vulnerability and the likelihood of its exploitation should be applied.

4- **Other Requirements**

4-1 The University must communicate with and subscribe to reliable cybersecurity sources that provide proactive information (Threat Intelligence), and cooperate with private groups with common interests and external experts on the topics

concerned in order to gather information about new threats and how to reduce existing vulnerabilities. (ECC-2-10-3-5)

4-2 The application of cybersecurity requirements to manage the technical vulnerabilities of King Faisal University should be reviewed periodically.

4-3 The Key Performance Indicator (KPI) should be used to ensure continuous development of vulnerabilities management.

4-4 This policy should be reviewed at least once a year.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity Unit.
- **Implementation of the policy:** the Cybersecurity Unit and the related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

17. Cybersecurity Incident and Threat Management Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards for managing KSC cybersecurity incidents and threats to reduce and protect cyber risks from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with cybersecurity requirements and related legislative and regulatory requirements, a legislative requirement in the item No. 2.13.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all information and technical assets of King Faisal University and is applied to all university employees.

Policy items

1- General requirements

1-1 The university must identify and detect cybersecurity incidents on time by providing the necessary techniques or by receiving and effectively managing communications from university employees or beneficiaries.

1-2 The University must proactively address cybersecurity threats by adopting preventive defenses to prevent or reduce the impact on the confidentiality, integrity or availability of information.

1-3 Cybersecurity incidents include but are not limited to:

1-3-1 Unauthorized changes on the user desktop and/or mobile device settings, and changes to server settings.

1-3-2 Malware infection.

1-3-3 Changes in applications appearance (unusual appearance) and modifications to user permissions such as upgrading access.

1-3-4 Unauthorized access to data, and/or modification without user permits or permissions.

1-3-5 Attempts to obtain information that can be used to carry out attacks, such as port scans, social engineering attacks, targeted scans across IP Range, etc.

1-3-6 Unauthorized activation of suspended or deleted user accounts.

1-4 The roles and responsibilities of the cyber incident response team, as well as important decision-making powers, the mechanism for communicating with internal and external actors as well as escalation mechanisms, must be all documented. (ECC-2-13-3-1)

1-5 If a cybersecurity incident is detected at the university, the incident response team must take the necessary steps to deal with the incident that was immediately discovered, which includes analyzing the incident data and determining its impact.

1-6 In case of a cybersecurity incident, relevant available information such as system and network records and other records from relevant security products (e.g. records from malware protection solutions, firewall, and advanced protection systems for detecting and preventing breaches) must be analyzed.

1-7 The significant evidence (for example, collecting evidence in accordance with legal restrictions and protecting it from manipulation) must be documented and protected so that it does not lose its usefulness in analysis. Then, it must be analyzed without destroying it or modifying its original image.

1-8 In case of a cybersecurity incident, the causes of the incident must be investigated and specialists such as Digital Forensics Analysts and cyber incident response teams should be called upon.

1-9 Cybersecurity incidents must be classified based on their severity and impact on the university's business (ECC-2-13-3-2).

1-10 Cybersecurity incidents are classified according to the table below (Table No. 4 - Classification of Cybersecurity Incidents):

Risk Level	Description	Response Time	Time to resolve the incident
Too High.	Serious damage directly affects King Faisal University's reputation and credibility, or affects many of its functional business units or business location significantly. It requires the activation of business continuity procedures.	Immediately	Two hours
High	A major outage affects functional business units, key services or location.	One or two hours.	4-5 hours
Moderate	An average impact on the functional business units, sites or IT assets, as well as an average-high impact on insignificant business units at King Faisal University.	2-3 hours	8-9 hours
low	A simple effect on a few resources, the incident can be tolerated for a certain period of time.	5 hours	24 hours

2- Cybersecurity Incidents Reporting

2-1 University staff must be raised security awareness and their responsibilities to cybersecurity incidents or threats by writing immediate report on any cybersecurity-related incidents or threats.

2-2 The university must identify an internal contact to report incidents either by phone or by email.

2-3 The university must identify incidents and threats that must be reported, when they should be reported, and parties that must be informed, such as the president and VP, the CEO of the Cybersecurity Unit, the in-house incident response teams. and the departments responsible for information and technical assets.

2-4 Before disclosing any information relating to security incidents to the third parties, the necessary approvals must be obtained in accordance with the relevant legislative and regulatory requirements.

2-5 Cybersecurity incidents must be reported to the National Cybersecurity Authority. (ECC-2-13-3-3)

2-6 The University should inform the National Cybersecurity Authority about the incident reports, indicators and reports of violations (ECC-2-13-3-4).

3- Responding to Incidents and Recovering from Cybersecurity Incidents

3-1 The cybersecurity unit's incident response team must write a report on the cybersecurity incidents, and the report must include the type and category of incident, personnel who reported the incident or the tools used to detect it, the services, assets or information affected, how the incident was detected, and any other documents or resources related to the incident.

3-2 Suppliers must be involved in the accident resolution or service recovery when needed.

3-3 Cybersecurity recovery procedures should include the identification Vulnerabilities exploited during the incident and use the necessary technical and administrative measures to resolve the incidents, for example:

3-3-1 Applying additional security controls (Compensating Controls).

3-3-2 Installing updates and fix packages.

3-3-3 Restoring system backups.

3-3-4 Resetting security systems settings, such as firewall system and penetration detection systems.

3-4 The Cybersecurity Unit must keep incident reports (including information about security vulnerabilities and incidents such as information about individuals, departments, specific systems, and/or attack methodology) in a safe place and restrict access to them.

3-5 The incident, if not resolved on time, should be escalated in accordance with the classification of incidents, the procedures for dealing with them and the escalation mechanism adopted.

3-6 If the treatment of the cyber incidents requires changes to the technical components, the university's change management procedures must be adhered to.

3-7 After resolving the incident, the Cybersecurity Unit's incident response team should hold meetings to discuss lessons learned with relevant departments to improve ways to deal with future cybersecurity incidents, as well as proactively deal with cybersecurity threats in order to prevent or minimize the effect on King Faisal University business.

4- Proactive Information on Threats

4-1 There must be cooperation with Threat Intelligence providers to continuously learn about and deal with incidents and threats related to cybersecurity. (ECC-2-13-3-5)

4-2 Proactive threat information should be saved and organized into a flexible and appropriate database to formulate work notes and indicator metadata such as knowledge base.

4-3 Advanced intrusion prevention and detection systems protection systems should be updated with proactive threat information and ensure that they can detect and deal with threats effectively.

5- Other requirements

5-1 Cybersecurity requirements for managing cybersecurity incidents and threats should be reviewed periodically. (ECC-2-13-4)

5-2 The Key Performance Indicator (KPI) should be used to ensure the continuous development of cybersecurity incidents and threats management.

5-3 This policy should be reviewed at least once a year.

Roles and responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation and implementation of the policy:** the Cybersecurity Unit and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

18. Database Security Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards for protecting King Faisal University databases to reduce and protect cyber risks from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with the cybersecurity requirements and related legislative and regulatory requirements, which is a legislative requirement in the item 1.3.2 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all database systems of King Faisal University and is applied to all university employees.

Policy Items

1- **General items**

1-1 All database systems used within the university must be identified, documented, and protected from environmental and operational risks.

1-2 Security technology standards for database systems inside the university must be developed and adopted and applied by database supervisors.

1-3 Except for database administrators, direct access or handling of databases for sensitive systems is denied, only through applications. (CSCC-2-2-1-8)

1-4 Access to databases is granted in accordance with the access ID management policy and permissions.

1-5 Copying or transferring databases of sensitive systems from the production environment to any other environment is prevented. (CSCC-2-6-1-5)

2- **Security Measures Required to Host Databases**

3-4 Identifying the business continuity and disaster recovery requirements for databases hosted in the contracts with the cloud service provider, which include mutual roles and responsibilities in terms of backup, incident response, disaster recovery plan, etc.

3-5 Providing logical isolation between university databases and other hosted databases.

3-6 The cloud-hosting site must be within the geographical area of Saudi Arabia. (ECC-3-3-2-4)

3-7 Restricting the administrative access to databases using an authorized encryption method such as the Secure Shell Home (SSH), Virtual Private Networks (VPN), or the Secure Sockets Layer (SSL)/Transport Layer Security (TLS), in accordance with the university's encryption policy.

3- Requirements for Managing Changes to Database Systems

3-1 Changes to databases (such as spreading databases, and moving to the production environment) must be made according to the change management process.

3-2 Updates and fixes are installed on the database system in accordance with the university's approved updates and repair package management policy.

3-3 Using reliable, approved and licensed database systems.

3-4 Ensuring the availability of a clear disaster recovery plan for database systems.

3-5 The university must sign a service level agreement for support with suppliers regarding the database management system in the production environment.

3-6 Applying retail and encryption to stored databases in accordance with the university's classification and encryption policy.

4- Monitoring Records of Events Related to the Database System

4-1 Activating and keeping event records for the database system in accordance with the university's event records management and cybersecurity monitoring policy.

4-2 The Cybersecurity Unit must monitor event records related to databases of sensitive systems, and monitor user behavior.

4-3 The Cybersecurity Unit must monitor and review the event records of database supervisors and monitor their behavior periodically.

5- Operational Requirements

5-1 Providing the necessary requirements for safe and appropriate operation of databases, such as providing a suitable and secure environment, restricting physical access to systems and allowing only authorized workers.

5-2 The relevant sections of the IT deanship must monitor operational database systems and ensure their quality of performance, availability, appropriate storage capacity, and so on.

5-3 Clock Synchronization is considered central and a reliable source for all database systems. (ECC-2-3-3-4)

6- **Other requirements**

6-1 Using the Key Performance Indicator (KPI) to ensure the continuous development of the database management system.

6-2 Reviewing the database management cybersecurity requirements at least annually or case of changes in legislative, regulatory or related requirements.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation and implementation:** the Cybersecurity Unit and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

19. Web Application Protection Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards for protecting King Faisal University's external web applications, to reduce and protect cyber risks from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with the requirements of cybersecurity and the relevant legislative and regulatory requirements, which is a legislative requirement in the item No. 2.15.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all external web applications of King Faisal University and is applied to all university employees.

Policy Items

1- **General Requirements**

1-1 External web applications purchased or developed internally must follow the multi-tier architecture principle. (ECC-2-15-3-2)

1-2 The principle of multi-level architecture should be used for external web applications for sensitive systems at least 3 levels (3-tier Architecture). (CSCC-2-12-2)

1-3 Ensuring that only secure communication protocols are used, such as hyper Security text Transfer Protocol (HTTPS), Security File Transfer Protocol (SFTP), TLS security, etc. (ECC-2-15-3-3)

1-4 Web Application Firewall (WAF) should be used to protect external web applications from external attacks. (ECC-2-15-3-1)

1-5 Development Environment and Testing Environment from the production environment must be applied.

1-6 Data and information protection techniques should be used in external web applications and in accordance with the data and information protection and classification policy.

1-7 In case of purchasing web applications from an external party, the supplier must adheres to the university's cybersecurity policies and standards.

1-8 At least minimum application security and protection standards (OWASP Top Ten) must be applied to external web applications for sensitive systems. (CSCC-2-12-1-2)

2- **Access Right Requirements**

2-1 Multi-Factor Authentication must be used for user access to external web applications. (ECC-2-15-3-5)

2-2 Security standards for web application development must be documented and adopted, including at a minimum secure session management, authenticity reliability, lockout, and timeout. (CSCC-2-12-1-1)

2-3 Access to production systems should be limited and controlled in accordance with functional responsibilities.

2-4 The security usage policy must be published for all users of external web applications. (ECC-2-15-3-4)

3- **Requirements for Developing or Purchasing Web Applications**

3-1 A cybersecurity risk assessment should be conducted when planning to develop or purchase web applications before they are launched in the production environment and in accordance with the university's cybersecurity risk management policy.

3-2 Before using protected information in the test environment, prior permission from the Cybersecurity Unit must obtained. Strict controls to protect that data, such as Data Scrambling and Data Masking technologies must be used and deleted immediately after they have been used.

3-3 Source Code must be securely saved. Only authorized employees are allowed to access it.

3-4 The penetration test for the external web application must be performed in the test environment and the results must be documented. It must be ensured that all vulnerabilities are addressed before launching the application into the production environment.

3-5 There should be a vulnerability test for the technical components of web applications and must be ensured they are processed by installing university-approved updates and repair packages.

3-6 Web applications must be approved by CAB before they are released in the production environment.

4- Other Requirements

4-1 Cybersecurity requirements for protecting external web applications should be reviewed periodically. (ECC-2-15-4)

4-2 The Key Performance Indicator (KPI) should be used to ensure continuous development to protect external web applications.

4-3 This policy is reviewed at least once a year.

4-4 Beneficiaries and users of the University's portal should have enough knowledge on the privacy and confidentiality policy in order to understand and agree with the type and nature of the data collected and analyzed.

4-5 Once the user visits the portal of the university, the portal management server records the user's IP, date and time of visit, address and link of any website browsed.

4-6 Protecting privacy in order to protect the personal information. It is recommended to:

* contact the cybersecurity unit immediately when it is likely that someone has been able to obtain the user's password, usage code, PIN, or other confidential information.
* not to disclose any confidential information over the phone or the Internet unless you confirm the identity of the person or party receiving the information.
* use a secure browser for online transactions while closing unused applications on the network, and making sure that the antivirus software is constantly up-to-date.
* contact the portal management via email on the site if there are any queries or opinions about the privacy policy.
* maintain your personal data, electronic storage as well as personal data sent are secured using appropriate security technologies.
* Notice that the portal contains links to websites or portals that may use ways to protect information and its privacy that differ from those used in the King Faisal University portal. The Cybersecurity Unit is; therefore, not responsible for the contents, methods and policies of the privacy of these other sites. It is recommended reviewing the privacy notifications of those sites.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** the Cybersecurity Unit and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

20. Cybersecurity Policy for Industrial Control Systems

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards relating to King Faisal University's industrial control devices and systems with the aim of reducing cyber risks and protecting them from internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with the cybersecurity requirements and related legislative and regulatory requirements, which is a legislative requirement in the item 5.1.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all the industrial control systems of King Faisal University and is applied to all university employees.

Policy items

1- **General Requirements**

1-1 All cybersecurity policies and requirements approved by the university and must be applied to industrial control devices and systems.

1-2 Strict restrictions must be imposed, and physical and logical division must be applied when linking industrial production networks with the University's internal business network (ECC-5-1-3-1).

1-3 Strict restrictions must be imposed, and physical and logical division must be applied when linking industrial production networks with external networks through the use of security control systems such as the Demilitarized Zone (DMZ) (ECC-5-1-3-2).

1-4 Logs Files cybersecurity event records must be activated on industrial networks and related communications. (ECC-5-1-3-3)

1-5 Safety Instrumented System (SIS) systems must be logically or physically isolated. (ECC-5-1-3-4)

1-6 Industrial Systems Security Updates and Repairs Packages (OT/ICS Patch Management) must be installed periodically in accordance with the University's Approved Updates and Repair Package Management Policy (ECC-5-1-3-7).

1-7 Vulnerabilities in industrial systems (OT/ICS Vulnerability Management) must be examined and detected periodically, and the vulnerabilities must be addressed based on their classification in accordance with the University's Approved Vulnerability Management Policy (ECC-5-1-3-8).

1-8 Access to the sites of industrial control devices and systems should be restricted and granted to authorized university employees only in accordance with the physical and environmental security policy and based on the requirements of their operational work.

1-9 A periodic examination of the effectiveness of backup recovery should be conducted and ensure that cybersecurity requirements for backup management are applied in accordance with the university's backup policy.

1-10 Data and information must be protected in the industrial control environment, and they should be handled based on their classification and in accordance with the university's classification policy.

2- Protection of Industrial Control Systems

2-1 Protection techniques must be provided to protect industrial control systems and devices from viruses and suspicious and harmful software.

2-2 Industrial control system network settings such as proxy servers, firewalls, and data Diodes devices must be adjusted to prevent unauthorized data transfer.

2-3 External storage media are prohibited from being connected to industrial control systems or technical components unless pre-authorized by the Cybersecurity Unit. (ECC-5-1-3-5)

2-4 The component settings of web-based industrial control systems should be adjusted as follows:

2-4-1 Using https protocol for authorized devices only.

2-4-2 Selecting and setting a specific list of applications (Whitelisting) to access web services.

2-5 The Web Applications Firewall (WAF) should be used to protect industrial control systems.

2-6 Multi-Factor Authentication must be used for access to users with important and sensitive powers over industrial control systems and devices.

2-7 Multi-tier Architecture must be applied in the development of web applications for industrial control systems.

2-8 Cybersecurity risks must be assessed periodically and in accordance with the university's cybersecurity risk management policy.

3- Managing Cybersecurity Incidents and Threats and Disaster Recovery

3-1 The mechanism for responding to cybersecurity incidents related to industrial control systems and escalation procedures must be determined.

3-2 Contingency Plan should be developed and adopted to keep the business running or it must be backed up from approved backups in case of cybersecurity incidents to ensure business continuity with minimal impact.

3-3 The disaster recovery plan for industrial control systems should be documented to include:

3-3-1 The required response to events of all periods and severity that leads to the activation of the disaster recovery plan.

3-3-2 Procedures for restarting or manually operating industrial control systems.

3-3-3 The roles and responsibilities of the response team and the list of employees authorized to have direct or indirect access to the industrial control systems.

3-3-4 Backup processes and procedures for backing up and storing information assets securely.

3-3-5 A complete and up-to-date logical network chart, and current settings information for technical components for industrial control devices and systems.

4- Other Requirements

4-1 The cybersecurity requirements of industrial control systems should be reviewed periodically. (ECC-5-1-4)

4-2 The Key Performance Indicator (KPI) should be used to ensure the continuous development of cybersecurity management related to the protection of the industrial control devices and systems.

4-3 This policy should be reviewed at least once a year.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** the Cybersecurity Unit and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

21. Encryption Policy

Objectives

The purpose of this policy is to provide best practice and standards-based cybersecurity requirements to ensure the proper and effective use of encryption to protect King Faisal University's electronic information assets and to reduce cyber and internal and external threats by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with the cybersecurity requirements and related legislative and regulatory requirements, a legislative requirement in the item 2-8-1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all the industrial control systems of King Faisal University and is applied to all university employees.

Policy items

1- **General items**

1-1 The University must develop, document and adopt encryption procedures and standards based on the need for its business and risk analysis and in accordance with the national encryption standards issued by the National Cybersecurity Authority. These procedure should include approved encryption solutions and limitations (technically and regulatory), methods of use, key issuance, deployment and recovery mechanism, and key backup management and encryption key destruction procedures. (ECC-2-8-3-1)

1-2 Data must be encrypted during transportation and storage based on its classification and according to the university's regulatory policies and procedures, and related legislative and regulatory requirements.

1-3 Updated methods, algorithms, keys and encryption devices must be used as issued by the National Cybersecurity Authority (CSCC-2-7-1-3).

1-4 All data on the sensitive systems must be encrypted during transportation (Data-In-Transit) (CSCC-2-7-1-1).

1-5 All sensitive systems data, during storage (Data-at-Rest), must be encrypted at the level of file and database or specific columns within the database (CSCC-2-7-1-2).

1-6 Roles and responsibilities related to key management infrastructure (KMI) should be identified and documented for at least the following roles:

1-6-1 Keying Material Manager.

1-6-2 Encryption supervisors responsible for protecting Key Custodians.

1-6-3 Certification Authorities (CAs), so that they are reliable and safe.

1-6-4 Registration Authorities (RAs) officials, so that they are reliable and secure.

2- Encryption Security Use

2-1 All encryption solutions (including algorithms, software, modules, libraries, and other encryption components) must be identified, evaluated and approved by the Cybersecurity Unit before being applied at the university.

2-2 Encryption must be applied in accordance with the university's encryption solutions.

2-3 Internally developed encryption algorithms must not be used in accordance with the Open Web Application Security Project Encryption Guide (OWASP).

2-4 Security verification methods (such as the use of public encryption keys, digital signatures and digital certificates) should be used to reduce cyber risks and in accordance with university's approved encryption solutions.

2-5 User identity verification must be used to transfer top-secret data to third parties using certified Digital Certificates, and in accordance with the Data Protection and Classification Policy.

2-6 Multi-Factor Authentication (MFA) must be used to verify the user's ability to access sensitive systems in accordance with the University's approved Data and Information Protection and Encryption Policy.

3- Encryption Keys Management

3-1 Encryption keys must be managed securely during key Lifecycle Management processes. They must be used properly and effectively. (ECC-2-8-3-2)

3-2 Encryption certificates must be issued by the university's internal certification authority for local services or by a reliable third party.

3-3 Private Key information must be kept in a secure place (especially if used for electronic signature), and unauthorized access, including certification authorities must be denied.

3-4 Technology must be provided to protect encryption keys when stored (Tamper Resistant Safe).

3-5 Private Key must be protected using a password and/or by storing them on a secure storage media, and in accordance with approved encryption procedures.

3-6 Private encryption keys must be classified as "Top Secret" information in accordance with the data protection and classification policy.

3-7 Event logs for encryption key management and monitoring solutions must be activated periodically.

3-8 The period of time and the date of creating and expiring the encryption keys must be specified.

3-9 Encryption keys must be renewed before they expire.

3-10 An updated Certificate Revocation List must be used to ensure that expired or security-violated encryption certificates are not used in the future transactions.

3-11 If the Private Key has been breached or not available (due to damage to key storage media), the certification authority must be immediately informed to cancel it and reissue the private key.

3-12 In case of a security breach, the certification authority must notify the university, cancel all certificates immediately, and replace the key.

3-13 If the encryption keys cannot be exchanged securely and reliably over communication networks, they must be transferred using secure and independent alternative channels (out-of-band channels).

3-14 Encryption key length requirements should be reviewed and updated based on the latest relevant technical developments at least once a year and in accordance with national encryption standards.

3-15 Encryption administrators are responsible for protecting Key Custodians and are only authorized to replace encryption keys when needed.

3-16 Encryption keys must not be saved on key memory or saved by the same systems as encryption. Instead, it is recommended that they be saved on independent devices Peripheral Hardware Devices such as Hardware Security Modules (HSM), Key Loaders, or any other dedicated devices.

4- **Other requirements**

4-1 The Key Performance Indicator (KPI) should be used to ensure continuous development of proper and effective encryption use.

4-2 All cybersecurity requirements for encryption should be reviewed periodically. (ECC-2-8-4)

4-3 This policy is reviewed at least once a year.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** the Cybersecurity Unit and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

22. Cybersecurity Risk Management Policy

Objectives

This policy aims to identify cybersecurity requirements based on best practices and standards for managing cybersecurity risks at King Faisal University, in accordance with considerations of the confidentiality, availability and integrity of information assets.

This policy follows national legislative and regulatory requirements and relevant international best practices, and is a legislative requirement as stated in the item 1.5.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all information and technical assets, industrial control systems and devices of King Faisal University and the work procedures of King Faisal University, and is applied to all university employees.

Policy items

1- **General items**

1-1 Cybersecurity Risk Management Methodology and cybersecurity risk management procedures must be developed, documented and adopted at the university. They must be aligned with the National Cybersecurity Risk Management Framework and internationally adopted standards and guidelines (e.g. ISO27005, ISO31000, and NET) to develop cybersecurity risk management methodology.

1-2 The cybersecurity risk management methodology should cover a minimum of:

1-2-1 Identifying the assets and know their importance.

1-2-2 Identifying and evaluating risks of the work, assets or staff of the university (e.g., the implications of King Faisal University resulting from cyber risks).

1-2-3 Identifying and evaluating cybersecurity threats and breaches that may affect information and technical assets.

1-2-4 Identifying ways to deal with cyber risks.

1-2-5 Arranging measures to reduce cyber risk by priority and in accordance with specific procedures.

1-2-6 Categorizing and defining cyber risk levels based on the level of impact and potential threat to the university.

1-2-7 Creating a cybersecurity risk record to document and follow up on risks.

1-2-8 Identifying roles and responsibilities to manage and deal with cybersecurity risks.

1-3 Risk assessment must be carried out periodically to ensure that information and technical assets are protected.

1-4 Cybersecurity Risk Management must be compatible with Enterprise Risk Management (ERM) at the university.

2- Phases of the Cyber Risk Management

2-1 Risk Identification: Cybersecurity Unit must identify events or circumstances that may violate the confidentiality, integrity and availability of information and technical assets, including, in particular, the identification of information and technical assets, potential threats and related breaches, and approved controls, thereby identifying the effects of the loss of confidentiality, integrity and availability of such assets.

2-2 Risk Assessment:

2-2-1 The Cybersecurity Unit must implement minimum cybersecurity risk assessment procedures in the following cases:

2-2-1-1 In the early stages of technical projects.

2-2-1-2 Before making a fundamental change in the technical structure.

2-2-1-3 When planning third-party services.

2-2-1-4 When planning and before launching new technical products and services.

2-2-2 Risks must be reassessed and updated as follows:

2-2-2-1 Periodically for all information and technical assets, and annually for sensitive systems. (CSCC-1-2-1-1)

2-2-2-2 After a cybersecurity incident that violates the integrity, availability and confidentiality of information and technical assets.

2-2-2-3 After obtaining important audit results or proactive information.

2-2-2-4 In case a change in information and technical assets.

2-2-3 The risk assessment process should cover:

2-2-3-1 Risk Analysis: The Cybersecurity Unit should assess the likelihood of threats and their effects, and use the results of this assessment to determine the overall level of these risks.

2-2-3-2 Risk Assessment :(Risk Evaluation) The Cybersecurity Unit should assess the magnitude of cyber risks in accordance with the university's ERM standards and prioritize how they are handled.

2-3 Risk Treatment:

2-3-1 The Cybersecurity Unit should identify risk management options by the following list:

2-3-1-1 **Risk Mitigation**: Treating or reducing the risk by applying the security controls needed to reduce the likelihood of occurrence, impact, or both, which help contain and maintain risks at acceptable levels.

2-3-1-2 **Risk Avoidance**: Eliminating risk by avoiding continuing with the source of the risk.

2-3-1-2-1 Risk Transfer: Sharing risks with a third party with the potential to deal with risks more effectively, or insuring information and technical assets if exposed to cyber risks.

2-3-1-2-2 Risk Acceptance: The risk level is acceptable, but should be constantly monitored in the event of a change.

2-3-2 Risk management options should be identified and documented based on risk assessment results, implementation cost and expected benefits.

2-4 Risk Oversight:

2-4-1 To track risks, the Cybersecurity Unit must prepare and maintain a risk record to document the outcomes of the risk management process.

2-4-1-1 The process of determining risks.

2-4-1-2 The scope of the risks.

2-4-1-3 The official or the risk-taker.

2-4-1-4 Description of risks including their causes and effects.

2-4-1-5 A risk analysis that shows the effects of risks and their time range.

2-4-1-6 Risk assessment and classification includes the probability, size and overall classification of risks if they occur.

2-4-1-7 The risk-handling plan includes the procedure, the person responsible for it, and its schedule.

2-4-1-8 Describing the remaining danger.

2-4-2 The Key Performance Indicator (KPI) should be used to ensure effective cybersecurity risk management.

2-4-3 The Cybersecurity Unit should collect and review evidence on the state of cyber risk periodically.

3- **Risk Appetite**

3-1 Risk appetite criteria must be defined and documented, depending on the level of the risk and the cost of addressing the risk.

3-2 Additional controls must be applied to reduce risk to an acceptable level if the remaining risk does not meet risk appetite criteria.

3-3 If the risk appetite criteria are exceeded, the authority must be informed to take the necessary actions or decisions.

4- **Other Requirements**

4-1 The methodology and procedures for managing cybersecurity risks should be reviewed and updated at planned intervals (or in the event of changes in legislative and regulatory requirements and relevant standards), and changes must be documented and adopted.

4-2 Cybersecurity risk management policy should be reviewed annually, and changes documented and adopted.

Roles and responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** Cybersecurity Unit.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

23. Cloud Computing and Hosting Cybersecurity Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards for protecting King Faisal University's information and technical assets on cloud computing and hosting services. This is to ensure that cyber risks are addressed or reduced by focusing on the basic objectives of protection: confidentiality, integrity and availability of information.

This policy aims to comply with the relevant cybersecurity and legislative and regulatory requirements, which is a legislative requirement in the item No 4.2.1 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all information and technical assets of King Faisal University on cloud computing services hosted, processed or managed by third parties, and is applied to all university employees.

Policy Items

1- **General items**

1-1 All third-party cybersecurity requirements in third-party cybersecurity policy apply to all cloud computing and hosting service providers.

1-2 The Cybersecurity Unit must verify the efficiency and reliability of the cloud computing and hosting service provider as well as obtain a license and an official register inside Saudi Arabia.

1-3 Cybersecurity requirements for cloud computing and hosting services must be applied in accordance with the university's regulatory policies and procedures and related legislative and regulatory requirements.

1-4 King Faisal University should conduct an assessment of the cybersecurity risks of hosting applications or services in cloud computing before selecting a cloud computing and hosting service provider.

1-5 The hosting site for sensitive systems, or any part of its technical components, must be inside the university or in cloud computing services provided by a government agency, or a national company that has achieved the National

Cybersecurity Authority's controls on cloud computing and hosting services, taking into account the hosted data classification (CSCC-4-2-1-1).

1-6 The Cybersecurity Unit should develop, document and adopt procedures for the use of cloud services.

1-7 Cloud and hosting provider contracts should include:

1-7-1 Cybersecurity requirements and Service Level Agreement (SLA) terms.

1-7-2 Non-disclosure Clauses, including the deletion and destruction of data by agreement between the service provider and the university based on the classification of such data and taking into account the data classification policy.

1-7-3 Business continuity and disaster recovery requirements.

1-7-4 The possibility of a university terminating service without justification or requirements.

1-8 The application of cybersecurity requirements with cloud computing and hosting providers should be reviewed periodically, at least once a year.

2- Cybersecurity Requirements for Data Hosting/Storage

2-1 Data must be classified before it is hosted or stored by cloud computing and hosting service providers (ECC-4-2-3-1).

2-2 Cloud computing and hosting service providers must return data (in usable form) and delete it unrecoverable upon termination or separation (ECC-4-2-3-1).

2-3 King Faisal University information must be signed, hosted and stored inside Saudi Arabia (ECC-4-2-3-3), taking into account regulations and legislative aspects that such data are not subject to any other country laws.

2-4 The Cybersecurity Unit should ensure that the university's environment (including virtual servers, networks and databases) is separated from other third-party environments in cloud computing services (ECC-4-2-3-2).

2-5 The cybersecurity unit must be approved to host sensitive systems or any part of its technical components.

2-6 King Faisal University should ensure that data privacy requirements are applied to data hosted in cloud computing.

2-7 Data and information transmitted to, stored, or transferred from cloud services must be encrypted in accordance with the relevant legislative and regulatory requirements at the university.

2-8 King Faisal University should ensure that the cloud computing and hosting service provider periodically backs up and protects backups in accordance with the university's backup policy.

2-9 The University should ensure that the cloud computing and hosting service provider cannot access stored data and that the service provider's access is limited by the permissions necessary to conduct and maintain hosting service management activities, or as required by business requirements.

2-10 The cloud computing and hosting provider must restrict access to the university's cloud services only to authorized users and by using User Authenticity methods in accordance with the university's access ID management policy and powers.

2-11 The cloud computing and hosting provider must provide the university with the technologies and tools to manage and monitor its cloud services.

2-12 The Cybersecurity Unit and the IT Project Management Office must coordinate with the university's legal affairs agency to include the terms of the cybersecurity requirements for hosting data in the contract with the cloud computing service provider.

3- **Other Requirements**

3-1 Ensuring that event records are activated on hosted information assets.

3-2 Cybersecurity event records must be monitored periodically.

3-3 Ensuring Clock Synchronization for cloud infrastructure with the university.

3-4 The Key Performance Indicator (KPI) should be used to ensure continuous development to protect information and technical assets on cloud computing services.

3-5 Cybersecurity requirements for cloud computing and hosting services should be reviewed periodically.

3-6 This policy should be reviewed at least once a year.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.

- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** the Cybersecurity Unit and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

24. Backup Policy

Objectives

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards related to ensuring that data, information and technical settings of King Faisal University's systems and applications are protected from damage caused by cyber risks, in accordance with king Faisal University's regulatory policies and procedures and related legislative and regulatory requirements. In addition, it provides a consistent framework for its application to the backup process to help prevent loss of KFU data by ensuring that data backups work properly when needed, whether it is simply to recover a particular file or when you need to fully recover the university's operating and application systems.

This policy aims to comply with cybersecurity requirements and related legislative and regulatory requirements, a legislative requirement in the item 2.9 Backup and Recovery Management of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope o and Applicability

This policy covers all procedures and processes of managing backups of King Faisal University systems and data, and is applied to all university staff.

Policy items

1- **General items**

1-1 Cybersecurity requirements should cover the basic requirements and controls of backup management (ECC-2-9-3) to a minimum:

* The scope and comprehensiveness of backups of sensitive information and technical assets.
* The immediate ability to restore data and systems after exposure to cybersecurity incidents.

1-2 Backup management should cover the cybersecurity requirements and controls of sensitive systems (CSCC: 2019) to a minimum:

* Backup Offline and Online to include all sensitive systems including data, information, and technical settings for the university's systems and applications.
* Backup at planned intervals based on risk assessment, and backup of sensitive systems is recommended on a daily basis.
* Securing access, storage and transportation of backup content and media for sensitive systems and protect them from unauthorized damage, modification or access.
* Conducting a periodic test at least every three months to determine the effectiveness of restoring backups for sensitive systems.

1-3 The application of cybersecurity-related regulatory requirements for backup management should be reviewed.

1-4 The most important data for the university's main sectors must be identified through the data classification process and by reviewing the assets of the information. The important and critical data must be identified so that they can be given higher priority during the backup process.

1-5 There should be a backup copy of:

* All data that the University decides are important and sensitive to the main business and activities of the university sectors and/or depending on the nature and functions of the employee.
* All data stored on the university's servers or data sharing service. Ehe employee is responsible for transferring his important data to the storage website.
* All data stored on network servers, which may include web servers, database servers, KFU Domain system controllers, firewall systems, and remote access servers.

1-6 Cybersecurity requirements must be identified, documented and adopted to manage backups.

2- **Backup Storage**

2-1 Backup media must be stored in a fire-resistant container and in an access control area and monitored by camera security surveillance systems.

2-2 The geographical distances between the backup preservation sites and the location of the University Data Centre must be maintained at an appropriate

distance to protect against fires, floods or other natural disasters, in order to ensure that no damage occurs in the event of a disaster at the main location of the data center.

2-3 When transferring or preserving backup media outside the main location of the data center, it must be ensured that they are not reasonably vulnerable to disasters such as theft or fires, and storage areas using environmental disaster protection methods must be selected and controlled for access to ensure the safety of backup media.

3- Repeating Backup

3-1 Backup should be performed at regular intervals.

3-2 The mechanism by which the backup process is repeated ensures that the data is successfully recovered. Appropriate backup dates must be scheduled to be consistent with the nature of the work of the university sectors and so that sufficient data can be recovered to continue working when there is a sudden accident, so that the pressure of work on users and the backup administrator can be avoided.

3-3 All university employees should know that each of them is personally responsible for their data on desktops or laptops in their custody. They should know that it is their responsibility to store all the important data they have on the university's backup and file sharing services.

3-4 Determining the level at which the information is necessary and backups must be stored.

3-5 Data recovery procedures must be tested and documented. The person responsible for the data recovery process should identified, how the data recovery is implemented and under what circumstances it must be implemented, and how long the entire process takes from request to data recovery. All these procedures must be clear and concise so that they are not confusing and misinterpreted in times of crisis by users other than backup officials.

4- Keeping Backup

4-1 Necessary time for keeping backup must be determined along with number of copies of the data stored to reduce risk efficiently while maintaining the required data.

4-2 Backups must be kept according to the save schedule and backup disposal. This schedule determines the status of the data as to whether it can be disposed of, recycled or kept in the archive store.

5- Stored Copies

5-1 Stored copies must be saved with a short description that includes the following information:

5-1-1 Backup history/resource name/backup method type (full/incremental).

5-1-2 A record of physical and electronic transactions must be kept for all backups, and the physical and electronic movement of the backups must indicate:

* The initial backup and the way it is transferred to storage.
* Any movement to back up from its storage site to another location.

5-2 Stored copies must be provided as soon as a certified request is received. The request for stored data must be approved by an authorized person, nominated by the Head of the Networks and Operating Systems Department at the IT deanship. Stored data requests must include:

* Filling out a form detailing the request, including the requested copy, where and when the applicant wishes to receive it and the purpose of the copy request.
* Acknowledge that the backup will be returned or destroyed as soon as it is completed.
* Showing a receipt as evidence that the backup has been returned.

5-3 An appropriate protection for information stored at the backup storage site must be provided in accordance with the standards applied at the main location of the data center. Controls applied to backup media at the main location of the data center should extend to the backup storage site.

6- Data Recovery Test

6-1 Backup recovery procedures must be checked and performed regularly to ensure their effectiveness and to ensure that recovery procedures can be completed on time and their ability to recover data can be reported.

6-2 Backup media must be tested regularly to ensure that they are relied on for emergency use.

6-3 Backup recovery must be tested when making any change that may affect the backup system.

6-4 Event log information resulting from each backup task should be reviewed daily for the following purposes:

* To check and correct errors.
* To monitor the duration of the backup process.
* To improve backup performance where possible.

7- Backup Media

Backup media must be protected from unauthorized access, misuse or tampering with them, including adequate protection to avoid any material damage arising during the transfer or storage process. All employees responsible for processing data backup must prove their identity and obtain permission to process those backups.

7-1 When special controls are needed to protect confidential or sensitive information, consider the following:

* Use secure storage (closet) places.
* Hand delivering.
* In critical cases, what will be delivered is divided into parts that send each part across a different means.

7-2 All backup media must be disposed of appropriately, as follows:

* Backup media must be equipped to get rid of them.
* Media should not contain backups (effective) so that they can be reused.
* You must ensure that current or previous media content is not accessed, read or retrieved by an unauthorized party.
* Backup media must be physically damaged so that their contents cannot be restored before they are disposed of.

7-3 Certain types of backup media have a limited career life as after a certain period of service they cannot be considered reliable. Consequently, the date should be recorded on them to be suspended after their use time exceeds factory specifications.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** the Cybersecurity Unit and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

25. Data and Information Protection and Classification Policy

Objectives

The purpose of this policy is to protect the data, stored data (electronic or paper records) held by King Faisal University and the persons who use it to ensure the protection of confidentiality, integrity, accuracy and availability of university data and information, in accordance with the university's regulatory policies and procedures, and the relevant legislative and regulatory requirements. This policy also identifies the basic requirements and responsibilities for proper management of data assets and determines the means of handling and transmitting data inside the university.

The policy also describes the principles for protecting information by determining how and to whom you can publish this information using a particular classification in order to maintain the privacy, integrity and availability of information assets at the university.

Scope and Applicability

This policy applies to all persons, systems, persons, and the ways of working. This includes all executives, committees, departments, partners, employees and other parties who have access to information systems or data created, collected, stored or processed at King Faisal University, whether electronically or non-electronically, regardless of where such data is located or the type of device stored. Therefore, it must be used by all employees and other parties that deal with the data held or owned by the university.

Policy items

1- General items

1-1 Information must be handled according to the specified classification in such a way that ensures the confidentiality, integrity and availability.

1-2 University data and information in sensitive systems handled by third parties must be classified in accordance with the National Cybersecurity Authority's Sensitive Systems Controls Document (CSCC-2-6-1-2).

1-3 Data and information protection technologies should be used in external web applications.

1-4 User Authenticity must be used to transfer top-secret data to third parties using certified Digital Certificates.

1-5 Private encryption keys should be classified as "top secret" information.

1-6 In all cases, there should be a reference to the controls of the National Documentation and Archives Centre for archiving, preservation and destruction of documents.

1-7 All King Faisal university data should be classified in one of the following:

* **Confidential (Restricted):** It defines confidential data as highly sensitive, and disclosing , losing or destroying them causes significant damage to one or more people or university authorities, and may include:
  - Personal data of university employees, students, university contracting companies or visitors: such as a user's email account, national identity/residence (Iqama) numbers, passport numbers, credit card numbers, driver's license numbers, or job/university number.
  - Authentication data: such as private encryption keys, username and password.
  - Financial records: such as financial account numbers.
  - Commercial materials: such as documents or data that are unique or specific intellectual property.
  - Legal data: including authorized data for legal authorities only.
* **Sensitive (Internal):** It refers to low-risk data that publishing , loosing or destroying it will not have a significant impact on people or university entities. It should not be published outside the university, and may include:
  - E-mail: most messages can be deleted or posted without causing damage (except e-mail received from people identified in the confidential classification).
  - Documents and files that do not contain confidential data.
  - Any data classified as non-confidential: It may include most business data, as most files managed or used daily can be classified as sensitive such as meeting minutes, action plans and internal project reports.
* **General (Unrestricted):** It refers to data that can be disclosed to the public and includes data and files that are not critical to the needs and processes of university work, which are deliberately published. It has neutral or positive impact on the university. This data may include media materials, advertisements, awareness materials, or marketing.

* Third parties must adhere to this data security classification whether they have a strategic partnership with the university or having a contract with the university.
* Accounting and financial records can be kept for at least 10 years.
* Annual audit reports and financial statements must be permanently maintained. Annual plans and budgets for the duration required to implement these reports must be retained and referenced when needed.

1-8 Contracts and correspondence related to contracts (including any modifications to the terms of the contract and all other supporting documents) must be retained.

1-9 The following records must be kept permanently :(meeting minutes, assignment orders, university seals, establishment provisions, regulations and permits).

1-10 Documents considered value can be destroyed after taking the necessary measures to record or summarize their data if they have been used or for another procedure in which they have been restricted for 10 years. Nevertheless, if they are under revision or examination, or required, or regulations or instructions of the Ministry of Finance, they are to be retained for a longer period.

2- **Electronic Documents:**

2-1 Electronic documents include Microsoft Office Suite, PDF files. Their data must be classified by the subject of the document. These documents also include images, drawings, engineering designs, charts, project models and templates, photo and video production files and other related files.

2-2 Keeping e-mail messages depends on their content. A saved email must be printed on a paper and kept in an appropriate file or uploaded and kept in digital form on personal computers.

3- **Legal Files and Documents:**

The university's legal archive is kept without specifying time as follows:

* Files of judicial proceedings and preliminary and final judgements, court decisions and orders and all relevant files.
* Legal notification and opinions issued by legal offices.
* Any other legal documents that the university's legal department believes should be preserved and archived.

4- Records:

4-1 The files of university employees and the documents they contain concerning their functions must be kept permanently even after the employee's contract with the university has been terminated.

4-2 Functional administrative records (including attendance and leaving records, application forms, change log, final service outcomes, student test results, training records) are kept as needed and according to the necessary duration estimated by the university.

4-3 Records and documents that university authorities have the right to determine how long they need to be retained. These records and documents are linked to the need of the university entities and liked to their use. These documents may include:

* Advisory reports.
* Policy and Procedure Guide (Original/Copy)
* Annual reports.

5- Document Destruction Procedures

5-1 Records should not be removed or destroyed unless they are classified to be eliminated or when their retention expires.

5-2 When records are kept during the specified period in retention schedule, they must be set up for destruction.

5-3 Financial documents are destroyed in accordance with the procedures specified by the relevant regulations issued by the General Department of Finance and Management.

5-4 Financial documents and personnel records are destroyed using tools that ensures complete destruction such as paper shredder machines.

5-5 Electronic data held in other media is disposed of by physically damaging those media.

5-6 The destruction of records must be done securely and completely.

5-7 The destruction must be recorded in the university's official data destruction document.

6- Data Storage

6-1 All electronic data is stored on the systems so that regular backups are allowed.

6-2 Employees should not be allowed access to data until they have been notified and agree to the terms of access to the data they would deal with.

6-3 Databases containing personal data have specific procedures for managing them and securing records.

7- **Data Disclosure**

7-1 If restricted data is shared with another party, be careful to disclose such data and to do so in a secure way.

7-2 When data is disclosed or shared, it must be done only in accordance with the documented data sharing protocol or data exchange agreement.

7-3 Disclosure of restricted data to any third party is prohibited without the consent of the authorized person.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Policy implementation:** the Cybersecurity Unit and all university entities.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

26. Physical and Environmental Security Policy

Objectives

The purpose of this policy is to define the basic rules for preventing unauthorized access and interference with KFU's information security facilities and systems. It aims at maintaining the security of information and employees from being exposed to various physical threats, which can adversely affect electronic systems and digital services or break them down. The university's information and technical assets are protected from unauthorized physical access, loss, theft and sabotage.

This policy aims to comply with cybersecurity requirements and related legislative and regulatory requirements, a legislative requirement in the item No 2.14 Physical Security of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy applies to employees of King Faisal University and any third party, whether they are working permanently or temporarily, regardless of their location, and covers all information systems environments operated by the University a third party.

Policy items

1- **Risk-based Physical Security Controls**

* The University must ensure that all its physical facilities have security factors in line with the risks of information systems in those facilities.
* All physical facilities at the university are identified and a security classification has been made.
* The physical and environmental security of the university's physical facilities is planned taking into account the degree of classification of information security and standards relating to the specific type of physical infrastructure of the University.
* The Department of Security and Safety at the university is responsible for applying the physical security controls to the buildings and facilities.

2- **Safe Areas**

* The university must develop the physical security scheme for its facilities. The university's physical plan must be distributed to areas so that each area has a

higher level of restrictions governing entry permit requirements. The surrounding areas can be classified as follows:

- Public area and reception area: (limited restrictions and subject to public monitoring).
- Office area: (Limited entry, visitors are checked-in and accompanied into this area. The area is publically controlled).
- Safe access area: (Limited entry, visitors are checked-in and accompanied into this area, supervised area)
- Restricted entry area: (limited to entry of authorized persons only) entry is subject to high restrictions, employees and visitors entering this area must have a specific entry permit, and this area is under control.
- Ensuring that information-processing facilities are not located in an environmentally unstable area.
- Ensuring that information-processing facilities are not close to any hazardous neighboring facilities (e.g. chemical laboratories, etc.).
- Ensuring that equipment used in emergencies and supporting copies is stored at a safe distance away from the main site to avoid exposure to the same incidents happening to main site.

3- **Physical Access Control**

* University employees, suppliers and contractors are allowed access to the university's physical facilities, including information processing facilities, only based on self-identification and identity verification in accordance with the procedures for granting material access.
* The activity/IT administrator supports access to safe and restricted areas. Access to areas with a high security rating, such as the Data Center, is limited to persons who have direct responsibility for the operation and maintenance of the Data Center.
* University employees, suppliers, contractors and other visitors should be required to wear a unique identification badge while they are in the university facilities permanently.
* Each visitor should sign the visitors' register. The visitor's name, company, purpose of visit, entry time, departure time and date must be documented in that register.
* It is strictly forbidden for employees to share the business access card to enter the working facilities.

* Telephone guides and internal documents used to locate sensitive processing facilities should not be placed in accessible place.
* All visitors must be accompanied by (a) university employee(s) while touring inside the safe areas.

4- **Checking Information Security Materials/ materials Entering and Leaving the Safe Areas**

* Materials entering and leaving the university must be checked before being transported from public access areas to its point of use.
* All transfer requests must be officially authorized by the information officer and recorded by physical security personnel.

5- **Maintenance of Physical and Environmental Security Infrastructure**

* The university must authorize the monitoring and controlling of any maintenance and diagnostic activities carried out locally or online.
* All maintenance should be monitored and relevant university employees should review maintenance records.

6- **Fire Protection**

* The Department of Security and Safety is responsible for responding to fire incidents and conducting fire handling exercises.
* Fire handling exercises should be conducted quarterly. These exercises should also be monitored, and all participants provided with statements regarding their contribution and performance.
* The Department of Security and Safety identifies critical locations that will be equipped with hand fire extinguishers. Noticeable cards should be placed on those areas and their location reported periodically to all employees during awareness training and the use of summary bulletins.
* The fire exit doors should be open only from the inside, and fire alarms should be prepared to be set up immediately when the emergency exit is opened, as part of the physical security measures required during fire evacuation.

7- **Monitoring Physical and Environmental Security**

* The University should ensure that its physical and environmental security controls are monitored in accordance with the risk classification levels of the relevant physical security environment.

* The Department of Security and Safety is developing a risk-based physical and environmental security control plan, which determines the physical and environmental security controls to be monitored and the responsibilities to be identified.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** cybersecurity unit, related departments at the Deanship of Information Technology, Security Management and Safety Management Department.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

27. Asset Management Policy

Objectives

The purpose of this policy is to ensure that King Faisal University has a precise and up-to-date inventory of assets that includes relevant details of all information and technical assets available at the University. The purpose is to support the university's operational processes and cybersecurity requirements, achieve the confidentiality, integrity, accuracy and availability of information assets, ensure that the university's information systems have been identified and assigned the officials to control them. These information systems should be appropriately classified in accordance with their nature and the classification of the security risks of information related to them. This classification helps to identify the appropriate security controls for those systems.

This policy also aims to comply with cybersecurity requirements and related legislative and regulatory requirements, a legislative requirement in the item 2.1 Asset Management of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cyber Security Authority. For more details, please refer to Section IV - Glossary of Terminology, at the end of this document.

Scope and Applicability

This policy covers all information systems environments operated by King Faisal University or a third party, and is applied to university employees and any third party, whether they are working permanently or temporarily, regardless of their location of work.

Policy Items

1- **General items**

* Information must be handled according to the specified classification to protect the confidentiality, integrity and availability of information.
* Cybersecurity requirements must be applied to manage information and technical assets.
* The Information and Technical Assets Appetite Policy must be identified, documented, adopted and published.
* The Information and Technical Assets Appetite Policy must be applied.

* Labeling and processing information and technical assets must be classified and handled in accordance with the relevant legislative and regulatory requirements.
* Cybersecurity requirements for information and technical asset management should be reviewed periodically.
* University data and information in sensitive systems handled by third parties must be classified in accordance with sensitive system controls (CSCC-2-6-1-2).
* Data and information protection techniques should be used in the university's external web applications.
* User ID verification should be used to transfer top-secret data to third parties using university-certified Digital Certificates.
* Private encryption keys should be classified as "top secret" information

2- **Defining Information Systems**

* Information systems are defined as technical and natural infrastructure that directly or indirectly affects the identification, processing, reporting, destruction and storage of university information. They include:
  - Information Technology applied programs.
  - Technical information processing infrastructure (computers and other information processing devices such as communications and smartphones, printers, etc.).
  - Network infrastructure and security.
  - Physical infrastructure (buildings, offices, meeting rooms, etc.).
  - Documents.
  - Other related infrastructure elements.

3- **Identify Information Systems**

All information systems at the University must be identified by conducting an inventory of these systems by the IT Deanship and the Information Security Department in accordance with information systems identification procedures (noting that the information collected in information systems records must be integrated into this inventory of information systems).

4- **Classification of Information Systems**

A rating score must be set for each university information system, taking into account the expected impact on the university's activity in the event of a breach of confidentiality, integrity or availability of the information system.

The information system administrator must classify information systems according to the university information systems classification, and in accordance with the procedures for classifying information systems.

5- **Placing Identification Cards on Information Systems**

The administrator of the information systems must place cards on each physical information system.

6- **Officials and Sponsors of Information Systems**

The responsible of the information system is the person or department who has the ultimate responsibility and has the permissions on the information system, and decides how and who will use the system.

The sponsor of the information system is the person or department who has been assigned for managing operations, changes, maintenance, and disposal of the information system with the authorization of the information officer.

The information system administrator is ultimately responsible for the security of that system.

The information security system sponsor, in cooperation with the Information Security Department, is responsible for implementing the controls required to provide security factors for that system.

7- **Updating the Inventory of Information Systems**

The inventory of information systems must be regularly reviewed and updated, if needed, in accordance with the university's information systems inventory procedures.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** cybersecurity unit, and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

28. Procurement Security Policy

Scope and Applicability

The University seeks to take advantage of the level of maturity achieved in the automation process and thereby reduce the operational costs associated with administrative financial transactions, while increasing technical support for systems at the level of all departments at the university. The role of cybersecurity in the procurement process is an integral part of the protection of sensitive data at the university sector, based on the response by mitigating the risks that may result from supply chain operations.

Policy items

All aspects of the potential risk of data breach must be secured.

The Department of Procurement and Tenders, as well as the General Department of Administrative and Finance Affairs and all other departments of the university dealing with the financial and administrative system, must determine the types of information that will be managed in the financial and administrative system. This information determines the permissions of those who will access the system are determined, and from which site they will reach it. In doing so, the team will have a better understanding of the potential risks.

All data transmitted between connected applications, including the financial and administrative system must be encrypted.

Ensuring the cloud-based services in order to take preventive action for network security, such as the use of security settings on firewall devices.

In addition, it must be ensured that security, protection controls are available in the financial and administrative system, and that it is secured and protected from distributed denial-of-service (DDoS) attacks that can lead to service interruptions.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** cybersecurity unit, and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.
- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

29. Information Non-disclosure Policy:

Scope and Applicability

The failure of university employees to implement the non-disclosure policy is considered a disclosure of university information that may be classified according to its degree of confidentiality. This should be regarded as a traffic accident for the leaking of information or data about government agencies and must be dealt with accordingly. In case of breach of confidentiality and non-compliance with non-disclosure agreements, the Cybersecurity Unit must be informed as soon as possible. The NDA form must be made available on the University's portal.

Policy items

Each contact must be with government agencies or regulatory authorities by relying on the university's communication and communication policy.

The employee must be authorized by his or her boss to make external contact.

All employees must also pass through the head of the department or the authority's administrator to find out the approved communication mechanism, and a specific protocol must be developed for this type of external communication.

With regard to information technology and information security, all contacts with external and private entities must be authorized by H.E. the Dean of Information Technology, chief executive officer of the university's cybersecurity unit, or any person authorized by the President of the university when needed.

Roles and Responsibilities

- **Sponsor and owner of the policy document:** CEO of the Cybersecurity Unit.
- **Policy review and update:** Cybersecurity unit.
- **Implementation of the policy:** cybersecurity unit, and related departments at the Deanship of Information Technology.

Adherence to the Policy

- The CEO of the Cybersecurity Unit, with the approval of his Excellency the President, must periodically ensure that all university bodies are committed to implementing and applying the cybersecurity policies and standards.
- All university employees must adhere to this policy.

- Any violation of this cybersecurity-related policy and policies is subject to a regular procedure in accordance with the regular procedures of the university and/or in accordance with the regular procedures issued by the relevant authorities.

Glossary

Terminology and Appendixes

1- Glossary

M	Term	Description of the term
1	Cybersecurity	Protecting networks, IT systems and operational technology systems; their hardware and software components: and their services: and their data, from any penetration; disruption; modification; entry; use or illegal exploitation.
2	Cyberspace	The interconnected network of IT infrastructure, which includes the Internet, communication networks, computer systems, Internet-connected devices, and associated hardware and controls.
3	Availability	Ensuring access and use of a reliably authorized user, procedure, or system when required.
4	Integrity	Protection against unauthorized modification or destruction of information, as well as ensuring that information is not denied and authenticity.
5	Confidentiality	The non-disclosure of information to an unauthorized user, procedure or system unless there is a permit for them to access it.
6	Information Assurance	Measures that protect information and information systems by ensuring their availability, integrity and authenticity, and not denying information and its confidentiality.
7	Accountability	The ability to track a particular activity or event until finding the responsible party. This is supported by non-denial, error diagnosis, detection and prevention of intrusions, and post-discovery procedures such as recovery and legal proceedings.
8	Authentication	Verifying the identity of the user, the process, or the body. It is often a prerequisite for allowing access to the technical resources.
9	Multi-Factor Authentication	A security system that checks the user's identity. It requires the use of several independent elements of identity verification mechanisms. These mechanisms include: - Knowledge, something the user knows, such as password. - Possession; the user owns, such as a program or device generating random numbers or temporary SMS messages to sign in, called one-time passwords - Inherent: a vital characteristic or characteristic related only to the user himself, such as fingerprint.
10	Authorization	Defining and confirming access rights/licenses to the authority's information and technical resources and assets in general, and controlling and confirming access levels in particular.
11	Asset	Tangible or intangible resources valuable to the entity.
12	Cryptography	Rules that include principles, means and methods for storing and transmitting data or information in a particular form in order to hide their semantic content, prevent unauthorized use and undiscovered modification so that unconcealed persons cannot read and process them.
13	Cybersecurity Resilience	The overall ability of the entity to respond to cyber incidents, absorb, and recover from damage in a timely manner.
14	Defense-in-Depth	Establishing multiple defensive levels of security controls by integrating people, technology, and operational capabilities
15	Cyber Attack	Illegal exploitation of computer systems, networks, and organizations whose work depends on digital information and communication technology to cause damage.
16	Distributed Denial of Service Attack	It is an attempt to disrupt the system and make its services unavailable by sending many requests from more than one source at the same time.
17	Phishing Email	Performing as a trustworthy entity by means of email messages to obtain sensitive information, such as usernames, passwords, or credit card details, for malicious and malicious reasons and intent.
18	Threat Intelligence	Organized information has been analyzed about recent, current, and potential attacks, which could be a cyber threat to the organization.

M	Term	Description of the term
19	Information Sharing	Sharing data and information, or knowledge, or both, for managing risks and threats or responding to cyber-attack.
20	Malware	A program that strikes systems with the aim of violating confidentiality, safety, availability of victim data, applications, or operating systems.
21	Ransomware	Malicious software that makes the victim's data and systems unusable until he pays money.
22	Disaster Recovery	Activities, programs and plans designed to return sensitive jobs and business services to normal after cyber attacks, or disruptions to these services and jobs.
23	Firewall	Hardware or software, limiting network data traffic, according to a set of access-enabling rules, which govern whether or not access is allowed.
24	Vulnerability	Any kind of vulnerability in the computer system, software or applications, or in a range of actions, making cybersecurity vulnerable to threat.
25	Vulnerability Assessment	Systematic screening of information systems or applications to determine the level of security controls, identify their shortcomings, provide data through which the effectiveness of security controls can be predicted, and ensure their efficiency after execution.
26	Penetration Testing	The process of testing a system, network, website, or smartphone application to detect breaches that can be exploited to carry out a cyber breach.
27	Traffic Light Protocol (TLP)	The Traffic Light Protocol is used to share the most sensitive information on a large scale in the world. There are four colors (light signals): red - personal and confidential for the recipient only, orange - limited participation, green - participation in the same community, white - unlimited.
28	Control No. 5-1-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements must be identified, documented and adopted to protect the devices and systems of industrial control (OT/ICS) of the entity."
29	Control No. 1.2.3 of the Basic Cybersecurity Controls (ECC-1:2018)	"A cybersecurity supervisory committee must be established under the guidance of the authority to ensure the commitment, support and track the application of cybersecurity programs and legislation, and members of the Committee, its responsibilities and business governance framework are identified, documented and accredited, with the head of the Cybersecurity Department being a member. It is preferable to be linked to the head of the entity or to those who alert it, taking into account the lack of conflict of interest. "
30	Control No. 1.3.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"The cybersecurity department must identify, document and approve cybersecurity policies and procedures and its cybersecurity controls and procedures, and publish them to relevant stakeholders."
31	Control No. 1.3.3 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity policies and procedures must be supported by security technical standards (e.g., security technical standards for firewall, databases, operating systems, etc.)."
32	Control No. 1.4.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"The authority must identify, document and adopt the regulatory structure of the authority's cybersecurity governance, roles and responsibilities, and assign the persons concerned. The support must be provided to enforce this, taking into account the lack of conflict of interest."
33	Control No. 1.5.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"The cybersecurity department must identify, document and adopt the methodology and procedures for managing cybersecurity risks in the region. This is in accordance with considerations of confidentiality and the availability and integrity of information and technical assets."
34	Control No. 1.6-2-2 of the Basic Cybersecurity Controls (ECC-1:2018)	"Reviewing the Configuration and Hardening and updating packages before launching projects and changes."
35	Control No. 1-6-3-1 of the Basic Cybersecurity Controls (ECC-1:2018)	Using 'Secure Coding Standards."
36	Control No. 1.6-3-5 of the Basic Cybersecurity Controls (ECC-1:2018)	" Reviewing the Secure Configuration and Hardening and updating packages before launching applications."

M	Term	Description of the term
37	Control No. 1.7.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"The authority must comply with national legislative and regulatory requirements relating to cybersecurity."
38	Control No. 1.8-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"The cybersecurity department in the authority should periodically review the application of cybersecurity controls."
39	Control No. 2-8-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"The application of cybersecurity controls in the entity must be reviewed and scrutinized by parties independent of the cybersecurity department (e.g. the audit department in the entity). The review and audit should be carried out independently, taking into account the principle of non-conflict of interest, in accordance with acceptable general standards of audit and relevant legislative and regulatory requirements. "
40	Control No. 1.9-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Employees must be identified, documented and adopted before, during their employment and at the end/termination of their employment in the entity."
41	Control No. 2.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"To ensure that the entity has an accurate and up-to-date inventory of assets that includes relevant details of all the information and technical assets available to the Authority, in order to support the authority's operational processes and cybersecurity requirements, in order to achieve the confidentiality, integrity, accuracy and availability of the entity's information and technical assets. "
42	Control No. 2.1-3 of the Basic Cybersecurity Controls (ECC-1:2018)	"The policy of Appetite of the authority's information and technical assets must be identified, documented, adopted and published."
43	Control No. 2.2.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements must be identified, documented and adopted to manage the entity's access identities and permissions."
44	Control No. 2.3.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements must be identified, documented and adopted to protect the agency's systems and information processing devices."
45	Control No. 2.3.3.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Virus protection, software, suspicious activities and malware on users' devices and servers using modern and advanced protection techniques and mechanisms, and safe management."
46	Control No. 2.3.3-3 of the Basic Cybersecurity Controls (ECC-1:2018)	"Manage patch management updates and repair packages."
47	Control No. 2.4.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements must be identified, documented and adopted to protect the entity's email."
48	Control No. No. 2-4-3-2 of the Basic Cybersecurity Controls (ECC-1:2018)	"Multi-Factor Authentication for remote access and access via the Webmail page."
49	Control No. 2.5-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements must be identified, documented and adopted to manage the security of the entity's networks."
50	Control No. 2.6-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"BYOD's cybersecurity requirements must be identified, documented and adopted when connected to the entity's network."
51	Control No. 1-8-2 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements for encryption must be identified, documented and adopted."
52	Control No. 2.9 of the Basic Cybersecurity Controls (ECC-1:2018)	"Ensuring that the data and information and the technical settings of the regulations and applications of the entity are protected from damage caused by cyber risks, in accordance with the regulatory policies and procedures of the authority, and the relevant legislative and regulatory requirements. :

M	Term	Description of the term
53	Control No. 2-10-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements must be identified, documented and adopted to manage the technical vulnerability of the entity."
54	Control No. 2.11.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements for penetration tests must be identified, documented and adopted."
55	Control No. 2.12-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"The requirements for managing event records and monitoring the cybersecurity of the entity must be identified, documented and adopted."
56	Control No. 2-13-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity incident management requirements and threats must be identified, documented and adopted."
57	Control No. 2-14 of the Basic Cybersecurity Controls (ECC-1:2018)	"Ensuring that the entity's information and technical assets are protected from unauthorized physical access, loss, theft and vandalism."
58	Control No. 2-15-1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements must be identified, documented and adopted to protect external web applications from cyber risks."
59	Control No. 4.1.1 of the Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements must be identified, documented and adopted within contracts and agreements with third parties."
60	Control No. 4.2-1 of the Basic Cybersecurity Controls (ECC-1: 2018)	"Cybersecurity requirements must be covered within contracts and agreements (e.g. SLA) with third parties that may be affected by the data of the entity or services provided to it."
61	(ECC-2-5-3-1) Basic cybersecurity controls (ECC-1:2018)	"Securing physical or logical isolation and division of network parts, necessary to control related cybersecurity risks, using firewall and defense-in-depth."
62	(ECC-2-5-3-8) Basic cybersecurity controls (ECC-1:2018)	"Protecting the Internet browsing channel from persistent advanced threats (APT Protection), which usually use and securely manage viruses and previously unknown malware.
63	(ECC-2-11-3-1) Basic cybersecurity controls (ECC-1:2018)	"The scope of penetration testing work, to include all services provided externally (via the Internet) and its technical components, including: infrastructure, websites, web applications, smartphone and tablet applications, e-mail and remote access."
64	(ECC-4-1-3-2) Basic cybersecurity controls (ECC-1:2018)	"Operations centers for operational and surveillance managing cybersecurity services, which use remote access, should be fully located inside the Kingdom of Saudi Arabia."
65	(CSCC-2-12-2) Basic cybersecurity controls (ECC-1:2018)	"The requirements for managing event records and monitoring the cybersecurity of the entity must be applied."
66	(ECC-2-15-3-1) Basic cybersecurity controls (ECC-1:2018)	"Using Web Application Firewall."
67	(ECC-2-15-3-2) Basic cybersecurity controls (ECC-1:2018)	"Using Multi-Tier Architecture."
68	(ECC-2-15-3-3) Basic cybersecurity controls (ECC-1:2018)	"Using secure protocols (such as HTTPS)."
69	(ECC-2-9-2) - Basic Cybersecurity Controls (ECC-1:2018)	"Cybersecurity requirements must be applied to manage the backup of the entity."
70	(CSCC-1-2-1-1) - CSCC-1 sensitive systems	"Implementing a cybersecurity risk assessment measure on sensitive systems, at least once a year."

M	Term	Description of the term
	cybersecurity controls: 2019)	
71	(CSCC-2-3-1-1) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Allowing only a specific list of Whitelisting files for applications and programs to work on servers for sensitive systems."
72	(CSCC-2-3-1-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Protecting servers for sensitive systems with end-point Protection technologies approved by the entity."
73	(CSCC-2-3-1-6) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Reviewing Secure Configuration and Hardening settings and fortifications at least every six months."
74	(CSCC-2-2-1-7) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Securing service account management of applications and systems; and disruption of interactive login through them."
75	(CSCC-2-2-1-8) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Except database administrators, direct access or interaction with databases of any user is prohibited; this is done only through applications, on the basis of their permissions, taking into account the application of security solutions that limit, or prevent database supervisors from accessing classified data."
76	(CSCC-2-3-1-1) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Allowing only a specific list of Whitelisting files for applications and programs to work on servers of the sensitive systems."
77	(CSCC-2-3-1-3) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Applying updates packages and security repairs, at least once a month to the sensitive external systems and internet-connected systems; and at least every three months to the internal sensitive systems, and following the agency's change mechanisms."
78	(CSCC-2-4-1-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Checking firewall settings at least every six months."
79	(CSCC-2-4-1-3) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Preventing direct connectivity for any device to the local network of sensitive systems, except after examination, and to ensure that the verified protection elements are available to acceptable levels of sensitive systems."
80	(CSCC-2-4-1-6) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Preventing sensitive systems from connecting to the Internet if they provide an internal service to the entity; there is no very necessary need to access the service from outside the entity."
81	(CSCC-2-4-1-8) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Protection against network disruption attacks (Distributed Denial of Service Attack "DdoS") to reduce the risk of network disruption attacks."
82	(CSCC-2-5-1-1) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Denial access the sensitive systems when using mobile devices, except only temporarily after a risk assessment has been carried out and the necessary approvals have been taken from the cybersecurity department in the entity."
83	(CSCC-2-5-1-2) - CSCC-1 sensitive systems	Performing "Full Disk Encryption for mobile devices which have the permissions to access to sensitive systems."

M	Term	Description of the term
	cybersecurity controls: 2019)	
84	(CSCC-2-6-1-1) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Non-Production Environment sensitive system data is only used after strict controls have been used such as Data Masking techniques or Data Scrambling techniques."
85	(CSCC-2-6-1-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Categorizing all sensitive systems data."
86	(CSCC-2-6-1-5) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Preventing the transfer of any production environment data of the sensitive systems to any other environment."
87	(CSCC-2-7-1-1) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Encrypting all sensitive systems data during (Data-In-Transit)."
88	(CSCC-2-7-1-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Encrypting all sensitive systems data during Data-At-Rest on the level of file, database, or column-specific data inside the database."
89	(CSCC-2-7-1-3) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Using up-to-date and secure methods, algorithms, algorithms, keys and encryption devices as issued by the Authority."
90	(CSCC-2-8-1) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Cybersecurity requirements must cover backup management."
91	(CSCC-2-8-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"A periodic testing must be conducted at least every three months to determine the effectiveness of restoring backups for sensitive systems."
92	(CSCC-2-9-1-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Assessing vulnerabilities and fixing them (by installing updates and repair packages) on the technical components of sensitive systems, at least once a month, for external, internet-connected sensitive systems; and at least every three months, for internal sensitive systems. "
93	(CSCC-2-9-1-3) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Immediate treatment of newly discovered Critical Vulnerabilities, with change management mechanisms adopted by the authority."
94	(CSCC-2-10-1-1) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"The scope of penetration testing work includes all technical components of sensitive systems, and all services provided internally and externally."
95	(CSCC-2-10-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Penetration testing must be done on sensitive systems, at least every six months."
96	(CSCC-2-12-1-1) - CSCC-1 sensitive systems	Secure Session Management includes authenticity, lockout and timeout. "

M	Term	Description of the term
	cybersecurity controls: 2019)	
97	(CSCC-2-12-1-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Applying and protecting the OWASP Top Ten standards at its minimum level."
98	(CSCC-2-12-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Multi-Tier Architecture must be used at least at the level (3-Tier Architecture)."
99	(CSCC-4-1-1-1) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Performing Screening or Vetting for attribution services companies, supporting service employees and managed services working on sensitive systems."
100	(CSCC-4-1-1-2) - CSCC-1 sensitive systems cybersecurity controls: 2019)	"Attribution services, services managed on sensitive systems; through companies and national destinations, in accordance with relevant legislative and regulatory requirements."

2- References

- Essential Cybersecurity Controls (ECC- 1: 2018), issued by the National Cybersecurity Authority - Document Access Link: https://nca.gov.sa/files/ecc-ar.pdf.
- Controls Cybersecurity Systems Controls (CSCC - 1: 2019), issued by the National Cyber Security Authority - Document Access Link: https://nca.gov.sa/files/cscc-ar.pdf.
- Dictionary of Cybersecurity Terminology, issued by the National Cybersecurity Authority - Link: https://nca.gov.sa/pages/glossary.html .
- Cybersecurity Toolkit Cybersecurity Policy Models, issued by the National Cybersecurity Authority - Link Models: https://nca.gov.sa/pages/kit.html.

- End of the document -

KFU

جامعة الملك فيصل

KING FAISAL UNIVERSITY

جـامعة ووطـن .. نمـاء .. واسـتدامة ..