King AbdulAziz University
Cyber-Security Center

Cyber-Security Roles and Responsibilities

Restricted-Internal

Document Authorization:

Role	Name	Date	Signature
Owner	Cyber-Security Center	14/11/2022 CE	

Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	30/10/2022 CE	Daniyal ibn Muhammad al-Ghazzawi	

Table of Contents

Introduction

This document has been developed to define responsibilities for implementing, supporting, and enhancing cyber-security programs and cyber-security requirements within the University. All parties involved in the implementation of cyber-security programs and cyber-security requirements must understand their roles and carry out their responsibilities relating to cyber-security at the University.

Objectives

This document aims to ensure that all parties involved in the application of cyber-security regulations at the University are aware of their responsibilities in regard to the implementation of cyber-security programs and cyber-security requirements at the University and at its affiliated entities.

This document aims to comply with cyber-security requirements and related legislative and regulatory requirements, which is itself a legislative requirement expressed in Controls 1-4-1 and 1-9-1 of the Essential Cyber-Security Controls (ECC-1:2018) promulgated by the National Cyber-Security Authority.

Roles and Responsibilities Related to Cyber-Security

The President of the University

No.	Responsibilities
1	Establishment of the Cyber-Security Center, ensuring its independence in such a way as to avoid conflicts of interests, and appointing the Director of the Cyber-Security Center, who must be a Saudi citizen.
2	Establishment of the Supervisory Committee for Cyber-Security.
3	Approval of the Governing Document of the Supervisory Committee for Cyber-Security.
4	Allocation of a budget sufficient for the requirements of cyber-security, including a budget for human resources.
5	Approval of the Strategy for Cyber-Security subsequent to its submission to the Supervisory Committee for Cyber-Security.
6	Approval of the Cyber-Security Policies subsequent to their submission to the Supervisory Committee for Cyber-Security.
7	Approval of the Cyber-Security Governance and Methodology for Managing Cyber-Risks documents subsequent to their submission to the Supervisory Committee for Cyber-Security.
8	Approval of the Cyber-Risk Management Methodology subsequent to its submission to the Supervisory Committee for Cyber-Security.
9	Reviewing reports concerning the state of cyber-security, and providing required support.

Members of the Supervisory Committee for Cyber-Security

No.	Responsibilities
1	Following up on principles and operational requirements in accordance with the Governing Document of the Supervisory Committee for Cyber-Security.
2	Providing a foundation for the principles of accountability, responsibility, and authority by defining roles and responsibilities with the aim of protecting the informational and technical assets belonging to the University.
3	Ensuring the existence of an approved methodology for managing and evaluating cyber-risks and the acceptable level of risk appetite at the University, and reviewing this methodology on an ongoing basis or when any fundamental change occurs in the acceptable level of risk.
4	Approval, support, and monitoring of cyber-security risk procedures.
5	Approval, support, and monitoring of cyber-security governance.
6	Review of the Cyber-Security Strategy in advance of its approval to ensure its compatibility with the strategic objectives of the University.
7	Approval, support, and monitoring of the implementation of the Cyber-Security Strategy.
8	Approval, support, and monitoring of the implementation of the Cyber-Security Policies.
9	Approval, support, and monitoring of cyber-security initiatives and projects (for example, the Cyber-Security Awareness Program, data and information protection, etc.)
10	Approval and monitoring of Key Performance Indicators, ensuring their effectiveness for the work of the Cyber-Security Center, and working to raise the level of performance.
11	Tracking and periodically monitoring reports on the management of data packets and settings.
12	Following up on and supporting the management of cyber-security incidents.
13	Reviewing the periodic reports produced by the Cyber-Security Center, which concern cyber-security projects, the general state of the cyber-security situation, internal cyber-risks that have the potential to affect the work of the University, and also external cyber-risks that may directly or indirectly affect the work of the University, and providing the necessary support to confront such risks.
14	Reviewing reports on cyber-security risks, tracking efforts to address them, and providing necessary support to efforts to address or reduce them.
15	Reviewing security reports on cyber-security incidents and making recommendations concerning them.
16	Reviewing requests for exceptions related to cyber-security and making recommendations concerning them.
17	Following up on the status of update packages and security fixes, assessing security vulnerabilities on all technical and informational assets, and ensuring these are addressed.

18	Reviewing the results of internal and external cyber-security assessments, ensuring the existence of an appropriate plan to address and track the observations detected, and providing the support necessary for addressing them.
19	Submitting periodic reports on the state of cyber-security, and providing requested support to the responsible authority.
20	Reviewing the state of compliance with the internal requirements of the University entity, and with the legislative requirements promulgated by the National Authority for Cyber-Security.

Director of the Cyber-Security Center

No.	Responsibilities
1	Supervising the development and updating of the Cyber-Security Strategy.
2	Supervising the development and implementation of methodologies and procedures for monitoring cyber-security incidents, directing and continuously tracking cyber-security activities, and submitting reports concerning them.
3	Supervising the development and updating of methodology and procedures for managing cyber-security risks.
4	Ensuring the development, approval, and implementation of cyber-security standards and procedures.
5	Supervising the development and updating of the Cyber-Security Policies based on present cyber-security requirements.
6	Ensuring the compatibility of cyber-security risk-management with risk-management at the University.
7	Providing solutions and recommendations on cyber-security to reduce cyber-risks to informational and technical assets.
8	Addressing issues related to planning and managing human resources that pertain to cyber-security (for example, recruitment, employee retention, and training), and providing necessary guidance and support in relation to these.
9	Supervising the identification and definition of cyber-security requirements in accordance with the relevant legislative and regulatory requirements and ensuring compliance with them.
10	Supervising and issuing reports concerning cyber-security response incidents.
11	Supervising the continuous assessment of vulnerabilities, and following up on the application of security update packages and settings.
12	Supervising the collection and analysis of prospective data relating to cyber-security, whether from national or international sources.
13	Supervising the execution of periodic penetration tests on all externally-provided services and their technical components in order to assess the level of cyber-security.
14	Supervising the preparation of cyber-security design principles and cyber-security designs for systems and networks, while ensuring alignment with the enterprise architecture.

15	Supervising the management of logical access to the University’s informational and technical assets by defining, documenting, and applying cyber-security requirements for managing access identities and powers at the University.
16	Supervising the preparation of the budget for the implementation of cyber-security initiatives and projects.
17	Ensuring the periodic review of cyber-security requirements.
18	Providing support and supervision to the preparation of an appropriate mechanism for measuring key performance indicators for cyber-security work, and sharing this mechanism with the Supervisory Committee for Cyber-Security.
19	Communication and relationship-management with the National Cyber-Security Authority.
20	Supervising cyber-security programs, including the Cyber-Security Awareness Program.

Cyber-Security Center Staff and Consultants

No.	Responsibilities
1	Development and annual review of cyber-security policies, procedures, and standards.
2	Definition, application, and review of methodology and procedures for managing cyber-security risks.
3	Ensuring the application of cyber-security policies, procedures, and standards.
4	Application and implementation of cyber-security risk-management processes.
5	Conducting risk assessments and monitoring the risk situation and measures taken in coordination with stake-holders.
6	Definition of responsibilities relating to risk in coordination with stake-holders.
7	Preparation of risk-assessment reports and obtaining their approval by the Cyber-Security Center.
8	Implementation and annual review of the Cyber-Security Compliance Program.
9	Development of the Cyber-Security Awareness and Training Program.
10	Implementation of the Cyber-Security Awareness and Training Program in coordination with the General Office of Human Resources, and assessment of the extent of employees’ compliance with cyber-security awareness.
11	Preparation of reports on compliance with the requirements of cyber-security, and obtaining their approval by the Cyber-Security Center.
12	Carrying out monitoring and reporting activities relating to cyber-security compliance.
13	Providing and monitoring the Cyber-Security Event Log Management and Monitoring System (SIEM).
14	Monitoring cyber-security monitoring systems to ensure their stability and availability, and submitting reports describing their status.
15	Collecting cyber-security events occurring in informational and technical assets in the Cyber-Security Event Log Management and Monitoring System (SIEM), analyzing logs, and identifying cyber-security risks.
16	Dealing with cyber-security incidents, following up on their resolution, and escalating existing incidents that exceed the defined Service Level Agreements.

17	Continuous assessment of vulnerabilities, and monitoring the application of security update packages and settings.
18	Conducting periodic penetration tests on all externally-provided services and their technical components to assess the cyber-security level.
19	Preparation of cyber-security design principles, cyber-security designs for systems and networks, and cyber-security architecture, while ensuring compatibility with the enterprise architecture.
20	Management of logical access to the University's informational and technical assets by defining, documenting, and applying cyber-security requirements for managing access identities and powers at the University.

Director of the Department of Information Technology

No.	Responsibilities
1	Ensuring the compliance of the Department of Information Technology with all cyber-security requirements.
2	Participation in and contribution to the development and application of risk management frameworks, procedures, and processes.
3	Employment of manual (non-automated) means for updates and repairs patches in the event that the automated tools in use at the University are not supported.
4	Periodic supervision and follow-up on the implementation of automated solutions for the management of update and repair patches.
5	Review of the effectiveness and efficiency of the management of updates and repairs to sensitive systems relating to information technology.
6	Ensuring the involvement of the Cyber-Security Center in all issues relating to informational and technical assets, project management, and procurement.
7	Ensuring the participation of the Cyber-Security Center in such a way as to guarantee the protection of the University's informational and technical assets as required.
8	Ensuring the review of current maintenance contracts with suppliers of informational technology systems and/or sensitive systems so as to equip the University with the latest versions of update and repair patches.
9	Monitoring the rate at which recommendations to reduce cyber-security risks are implemented.
10	Supervising the management of operational processes for technical assets relating to cyber-security.

Staff of the Department of Information Technology

No.	Responsibilities
1	Application of cyber-security requirements relating to the Department of Information Technology, including the Cyber-Security Policies and cyber-security procedures, processes, standards, and guidelines.
2	Addressing vulnerabilities and monitoring the application of security update packages and settings.

3	Application of cyber-security requirements as they relate to the nature of the work of the employees concerned.
4	Reporting any suspicious activities or cyber-security concerns and escalation of them to the Cyber-Security Center.
5	Assisting in providing inputs to risk-management framework activities and related documentation.
6	Coordination with the Cyber-Security Center on all issues relating to informational and technical assets and project management.
7	Coordination with the Cyber-Security Center to ensure the protection and security of the University's informational and technical assets as required.
8	Review of current maintenance contracts with suppliers of informational technology systems and/or sensitive systems so as to equip the University with the latest versions of update and repair packages.

Parties Responsible for Application Development

No.	Responsibilities
1	Supervising the implementation of the cyber-security requirements promulgated by the University's Cyber-Security Center relating to the development of applications, specifically for those applications that the University controls.
2	Coordination with the Cyber-Security Team on cyber-security-related issues that affect the University's applications.
3	Supervising the application of the cyber-security standards adopted by the Cyber-Security Center for application development, such as the Open Web Application Security Project (OWASP).
4	Ensuring the documentation of the source code for internal and external (i.e. through an external party) development processes for applications within the University entity, so as to enable the University's Cyber-Security System to undertake tracking and review processes for the management of vulnerabilities.
5	Ensuring secure programming within the mechanisms for constructing applications, by ensuring that errors are addressed and potential errors are identified, in order to limit vulnerabilities in accordance with the policies communicated by the University's Cyber-Security Center.
6	Ensuring that all vulnerabilities reported by the University's Cyber-Security Center are addressed in the software acceptance phase, including completion criteria, risk acceptance and documentation, common criteria, and independent testing methods, and notifying the Cyber-Security Center concerning them.
7	Coordinating with the University's Cyber-Security Center to identify services and functions related to cyber-security at the level of applications, and employing these to limit opportunities for exploitation.

Developers of the University’s Applications

No.	Responsibilities
In addition to the responsibilities mentioned for the University Portal Applications Management staff, those involved in developing applications have the following responsibilities:	
No.	Responsibilities
1	Implementation of cyber-security requirements related to the development of the University’s applications in accordance with the standards and procedures for the development of applications communicated by the Cyber-Security Center (for example, standards for the secure development of applications).
2	Implementation of project tasks and changes to software development projects within the University entity.
3	Identification and documentation of necessary updates and fixes for software.
4	Executing secure programming, and addressing errors and identifying potential errors in code to limit vulnerabilities, in accordance with the policies and mechanisms communicated by the University’s Cyber-Security Center.
5	Identifying and documenting updates and fixes needed for software, and versions that leave software open to vulnerabilities.

Administrators of Infrastructure and Projects Offices in the Department of Information Technology

No.	Responsibilities
1	Coordination, planning, and scheduling maintenance periods according to priority in order to install update and repair patches, in accordance with the Projects and Modifications Management Policy adopted by the University, in a way that does not negatively affect the cyber-security of assets.
2	Supervising automated solutions for the management of update and repair packages, and ensuring the execution of manual updates in the event that automated update and repair patches are not supported.
3	Supervising regular backups and backup tests.
4	Supervising the implementation of cybersecurity requirements related to information technology processes at the University.
5	Ensuring that update and repair patches for informational and technical assets are tested prior to propagation.
6	Ensuring that update and repair patches are successfully installed onto systems.
7	Ensuring the implementation of cyber-security policies relating to informational and technical assets belonging to the University (for example, the User Device Security Policy form, the Server Security Policy form, etc.).
8	Determination and arrangement of priorities and capabilities for the restoration of systems and required basic operations units, in whole or in part, subsequent to a catastrophic event affecting systems and operations continuity.

9	Determination of appropriate levels of information availability on systems, based on the basic functionality of the system in question, while ensuring that the system requirements specify the requirements for disaster recovery and operations continuity, including any fail-over site requirements, backup requirements, and support capability requirements, so as to support system restoration and recovery.
10	Supervising tests of the efficiency of the Disaster Recovery Plan, and participating in tests of the efficiency of the Operations Continuity Plan.

Parties Responsible for Infrastructure Management Offices in the Department of Information Technology

No.	Responsibilities
In addition to all of the responsibilities mentioned for employees of the Department of Information Technology, those concerned with information technology processes bear the following responsibilities:	
1	Assistance in coordinating with the Cyber-Security Center on issues relating to cyber-security that affect the Office of Information Technology Processes.
2	Implementation of cyber-security requirements relating to information technology processes at the University.
3	Implementation of automated solutions for the management of update and repair patches.
4	Provision and periodic testing of backup versions.
5	Implementation of automated solutions for the management of update and repair patches, and ensuring that manual updates are performed whenever automated update and repair patches are not supported.
6	Creation and protection of appropriate records, and integration of these into the Central Records Management System.
7	Configuration of all management software, protection software, and operating systems for informational and technical assets.
8	Supervision of access powers and user accounts for informational and technical assets in accordance with specified policies.
9	Compliance with the isolation of informational and technical assets and the logical division of network elements in a secure fashion.
10	Participation in the management of threats and incidents in the information technology system at the relevant stages (for example, the stages of containment, eradication, and recovery).
11	Assisting with the identification and prioritization of systems capabilities and basic operations units required for full or partial restoration of specific systems subsequent to a catastrophic event that causes a cyber-security failure.
12	Assisting with determining appropriate levels of information availability in systems, based on the underlying functionality of the system in question, while ensuring that the system requirements specify the requirements for disaster recovery and operational continuity, including any fail-over site requirements, requirements for

	backup versions, and support capability requirements for system restoration and recovery.

General Director of the General Office for Human Resources

No.	Responsibilities
1	Supervising the implementation of cyber-security requirements relating to human resources at the University.
2	Ensuring that security surveys are conducted for employees in cyber-security jobs and in technical positions holding important and sensitive powers, in coordination with the relevant offices.
3	Assuming responsibility relating to support for the application of the Acceptable Use of Assets Policy, and applying penalties to violators of the Policy in accordance with the procedures adopted by the University.
4	Assuming responsibilities relating to the Human Resources Cyber Security Policy that follow on from update and review of the policy.
5	Attending and participating in meetings of the Supervisory Committee for Cyber-Security as necessary.
6	Requesting adequate funding for training resources relating to cyber-security, including in-house courses and courses relating to the sector, instructors, and related materials.
7	Carrying out educational needs assessments and identifying requirements relating to cyber-security.
8	Ensuring the preparation and implementation of standardized job roles and responsibilities in accordance with well-defined occupational roles relating to cyber-security.
9	Definition of cyber-security career paths to allow opportunities for professional growth and promotions in professional fields relating to cyber-security.
10	Coordinating with the Cyber-Security Center on issues relating to cyber-security that affect the Office of Human Resources.
11	Participation in and providing inputs concerning the review of the Cyber-Security Strategy and Policies.
12	Dealing with non-compliance violations of cyber-security policies, in coordination with the General Office of Legal Affairs.

Staff of the General Office of Human Resources

No.	Responsibilities
1	Implementation of cyber-security requirements relating to human resources at the University.
2	Conducting security surveys for employees in cyber-security jobs and in technical positions holding important and sensitive privileges, in coordination with the relevant offices.

3	Conducting an assessment of the security awareness of all employees, identifying points of weakness relating to cyber-security, and working to address these.
4	Conducting the Cyber-Security Awareness and Training Program in coordination with the Office of Cyber-Security Awareness and Training.
5	Preparation and implementation of standardized job roles and responsibilities in accordance with well-defined occupational roles relating to cyber-security.
6	Assistance in defining cyber-security career paths to allow opportunities for professional growth and promotions in professional fields relating to cyber-security.
7	Providing support for requesting adequate funding for training resources relating to cyber-security, including in-house courses and courses relating to the sector, instructors, and related materials.

Director of the Governance, Risk-Management, and Compliance Unit at the Cyber-Security Center

No.	Responsibilities
1	Overseeing the periodic audit and assessment of cyber-security programs and requirements in accordance with generally-accepted auditing standards and relevant laws and regulations.
2	Supervising cyber-security audits in accordance with the terms of the Cyber-Security Assessment and Review Policy.
3	Ensuring the periodic review and updating of all documents relating to cyber-security.
4	Attending and participating in meetings of the Supervisory Committee for Cyber-Security as needed.
5	Ensuring that cyber-security risks are updated and re-evaluated in accordance with the Cyber-Security Risk-Management Policy.
6	Ensuring that risk-acceptance is aligned with the Cyber-Security Risk-Management Policy.
7	Proposal of plans to address audit results and observations.
8	Documenting audit results and observations, and reporting them to and discussing them with the relevant offices.
9	Submission of audit results and observations to the Supervisory Committee for Cyber-Security.
10	Discussion of corrective actions with those responsible for audit results, and documentation of these discussions.
11	Reporting any ineffective controls relating to cyber-security.
12	Reporting non-compliance with cyber-security requirements.
13	Coordination with the Cyber-Security Team on cyber-security issues that affect the Internal Assessment Office.
14	Reviewing the Cyber-Security Strategy and Policies and providing input concerning them.

Staff of the Governance, Risk-Management, and Compliance Unit at the Cyber-Security Center

No.	Responsibilities
1	Assisting with the assessment and audit of the implementation of cyber-security controls in accordance with generally-accepted auditing standards and relevant laws and regulations.
2	Implementation of cyber-security requirements relating to audits internal to the University.
3	Periodic review and updating of all documents relating to cyber-security.
4	Conducting reviews to ensure that cyber-security risks are updated and reassessed in accordance with the Cyber-Security Risk-Management Policy.
5	Conducting reviews to ensure the alignment of risk-appetite with the Cyber-Security Risk-Management Policy.
6	Conducting reviews and reporting non-compliance with cyber-security requirements to the Head of the Office for Internal Assessments.
7	Implementing the cyber-security assessment process in accordance with the terms of the Cyber-Security Assessment and Audit Policy.
8	Analysis of cyber-security controls in effect, and making recommendations to the Head of the Office for Internal Audits concerning them.
9	Suggesting corrective procedures to the Head of the Office for Internal Audits in accordance with the results and observations of assessments.
10	Assisting with proposals for plans to address the results and observations of audits.
11	Assisting the Cyber-Security Team on cyber-security issues affecting the Office of Internal Audits.

General Office for Legal Affairs

No.	Responsibilities
1	Compiling national regulatory and legislative requirements relating to cyber-security, as well as domestically-approved international agreements that include requirements pertaining to cyber-security that apply to the University.
2	Translating cyber-security controls, regulations, policies, standards, and procedures, and rendering them legally binding.
3	Ensuring that terms and conditions and non-disclosure policies are binding upon staff and external parties in order to protect the informational and technical assets of the University.
4	Supervising the implementation of cyber-security requirements relating to legal affairs at the University.
5	Attending and participating in the meetings of the Supervisory Committee for Cyber-Security as needed.
6	Evaluating the effectiveness of cyber-security laws and regulations.

7	Reviewing the External Parties Security Policy adopted by the University in accordance with relevant legal requirements.
8	Working with the Cyber-Security Center on cyber-security issues that affect the Office of Legal Affairs.
9	Providing support in addressing cyber-security incidents as needed.

Staff of the General Office for Legal Affairs

No.	Responsibilities
1	Assisting in the interpretation and application of cyber-security laws, regulations, policies, standards, and procedures with regard to specific issues.
2	Implementation of cyber-security requirements as they relate to legal affairs at the University.
3	Assistance in evaluating the effectiveness of cyber-security laws and regulations.

All Workers

No.	Responsibilities
1	Dealing with all data and information in accordance with its level of classification.
2	Avoiding the infringement of the rights of any person or company protected laws pertaining to copyright, patent, or other types of intellectual property, or similar laws or regulations.
3	Adherence to cyber-security policies and procedures.
4	Adherence to cyber-security requirements relating to user device protection.
5	Adherence to cyber-security requirements relating to the use of the Internet and software.
6	Adherence to cyber-security requirements relating to e-mail.
7	Compliance with requirements relating to cyber-security protection systems and technologies.
8	Using any and all of the University's informational and technical assets for work purposes only, and in accordance with the Acceptable Use of Assets Policy adopted by the University.
9	Obtaining the required permit from the General Office of Security Services, or from the University Authority, prior to hosting visitors at sites designated as sensitive by the University.
10	Reporting cyber-security incidents.
11	Adherence to the Acceptable Use Policy.

Roles and Responsibilities

Responsible Party and Owner of the Document: Director of the Cyber-Security Center.
Updating and Review of the Document: The Cyber-Security Center.

Implementation and Application of the Document: The Cyber-Security Center and the General Office for Human Resources.