Table of Contents

Issue Control

Change Approval	This document may be viewed, printed by authorized personnel only. Any changes to this policy shall be reviewed and accepted by the IT Deanship and approved by Information Security Manager.
Review and Update	A policy review shall be performed at least on an annual basis to ensure that the policy is current. It is the responsibility of the Information Security Manager to facilitate the review of this policy on a regular basis. Personnel and Department Head from Relevant Departments shall also participate in the annual review of this Policy.

Policy Structure

1.Purpose

This policy is to empower, within KAU, the Information Security Department to perform information security Risk Management for the purpose of determining areas of vulnerability, threats and to initiate appropriate remediation.

2.Scope

This policy applies to KAU and all parties, its affiliated partners, companies or subsidiaries, including data processing and process control systems, that are in possession of or using information and/or facilities owned by KAU.

This policy applies to all staff/ users that are directly or indirectly employed by KAU, subsidiaries or any entity conducting work on behalf of KAU that involves the use of information assets owned by KAU.

3.Role and Responsibilities

Based on KAU's Organizational Structure, the following is a list of roles and their associated responsibilities towards this policy.

1. IT Deanship Role

- Distribute information security documents so that those who need such documents have copies or can readily locate the documents via an intranet site.
- Ensure the protection of information/infrastructure systems, according to the technological mechanisms defined by the system / application design team.
- Perform system/application/network security monitoring.

2. Information Security Department Role

- Define and maintain the information security policies.
- Prepare and periodically updates information security manuals needed to advance information security at KAU.
- Implement appropriate controls to protect the confidentiality, integrity and authenticity of sensitive information.

3. Information Asset Owner Role

- Protect, manage critical information assets, for which he has been assigned as an Information Owner.
- Determine the access rights of users to information assets.

4.Compliance

Compliance with this policy is mandatory and KAU division managers must ensure continuous compliance monitoring within their divisions. Compliance with the statements of this policy is a matter of periodic review by Information Security Manager and any violation of the policy will result in corrective action by the Information Security Committee with cooperation with relevant security entities. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets.
- Actions like Financial/monetary penalty, termination of the employee or downgrading from the existing position as deemed appropriate by IT Dean, Administration Department, and the Legal Division.

5.Waiver Criteria

This policy is intended to address information security requirements. If needed, waivers could be formally submitted to the Information Security Department, including justification and benefits attributed to the waiver, and must be approved by KAU Information Security Steering Committee.

The policy waiver period have maximum period of one year, and can be reassessed and re-approved, if necessary for maximum three consecutive terms. No policy should be provided waiver for more than three consecutive terms.

6.Related Policies

- Compliance Policy.
- Asset Management Policy.
- Access control Security Policy.
- Business Continuity Planning Policy.
- Personnel Security Policy.

7.Owner

- Information Security Manager.

8. Policy Statement

To ensure cost effective assets protection and business operation continuity KAU shall define and implement risk management. Risk management shall be conducted for all the assets owned or entrusted to KAU. As a result of the risk management KAU shall develop and implement all the countermeasures to reduce and/or mitigate all the risks.

1. Risk Assessment Methodology

Policy Objective	Policy Statement
Identify, analyze, and evaluate organization risks	➢ The risk methodology shall consider of the following elements: • Identifying assets and identify which are most critical. • Identifying, characterizing, and assessing threats. • Assessing the vulnerability of critical assets to specific threats. • Determining the risk (i.e. the expected consequences of specific types of attacks on specific assets). • Identifying ways to reduce those risks. • Prioritizing risk reduction measures based on a strategy.

2. Risk Management Documentation

Policy Objective	Policy Statement
Realize potential opportunities whilst managing adverse effects	➢ KAU shall prepare an appropriate documentation in order to manage any risk properly. ➢ Information Security Manager shall review and approve the risk management and documentation. ➢ Assets owners shall maintain risk registers as risks impact on their respective responsibilities. Information from these registers shall be given to the Information Security Manager who shall develop and maintain KAU risk register. ➢ All information risk management documentation shall be treated as restricted information, delivered to and retained by the IT Deanship.

3. Assessment of Risks

Policy Objective	Policy Statement
Conduct risk assessment in all organization assets	➢ A risk assessment shall be performed on all existing and new infrastructure in accordance to the risk management methodology. ➢ Risk assessment shall be embedded in ongoing business or technical operations. ➢ The Risk assessment shall be conducted for new existing contracts and any changes to contract. ➢ Risks shall be identified based on threats and vulnerabilities of the KAU key assets.

4. Risk Mitigation

Policy Objective	Policy Statement
Reduce risk by implementing the cost-effective security measures	➢ The risk mitigation process shall consider the following: • Selecting the appropriate countermeasures that will reduce exposure to the risk. • Assigning a priority ranking to the implementation of the countermeasures. • Assigning financial and technical responsibility for implementing the countermeasures. • Implementing and documenting the countermeasures and safeguards.

5. Risk Acceptance and Residual Risks

Policy Objective	Policy Statement
Ensure that risk is been accepted through a formal process	➢ KAU shall follow a formal process for accepting risk by deciding to accept the existing risk and /or the residual risk and acknowledging that some risk exists even after cost-effective countermeasures have been implemented. ➢ If the level of residual risk is not acceptable, then further countermeasures shall be implemented to reduce exposure to acceptable levels.

6. Risk Management Training and Awareness

Policy Objective	Policy Statement
Ensure that all relevant people are aware of the risk management	➢ Information Security Department shall conduct risk assessment training and awareness to ensure that all relevant management and staff understand and implement the Risk Management controls and requirement.

7. Risk Management Monitoring and Reviewing

Policy Objective	Policy Statement
Monitor the implementation of risk management	➢ Internal Audit Program shall be annually performed to monitor the implementation of this policy. This audit shall assess whether: • The risk management plans are in place for the function being audited. • The risk management plans are appropriately integrated with other planning documents; are current and reviewed on a regular basis. • Internal Audit, as part of normal post audit reporting, shall report on risk management issues to management and other relevant parties.

8. Re-Assessment of Risk

Policy Objective	Policy Statement
Update the risk assessment with the new changes	➢ The risks shall be re-assessed and updated as follows: • At least every two years following the last risk assessment. • After a significant audit finding. • Whenever the infrastructure experiences significant enhancement or modification. ➢ After an information security incident that violates an explicit or implied security policy and compromises the asset's integrity, availability, or confidentiality

9. Independent Risk Management

Policy Objective	Policy Statement
Ensure the risk management is evaluated by independent party	➢ Independent risk management shall be conducted by organizations that are separate and distinct from those responsible for the development and operation of the information. ➢ Independent processes (e.g., independent risk assessment, independent code review, independent security test validation, independent penetration testing and vulnerability scans) shall be conducted by independent personnel, contractors, or vendors for the purpose of applying rigorous evaluation standards to information.

Glossary

Asset Anything that has value to the organization

Availability The property of being accessible and usable upon demand by an authorized entity

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Control Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature

Note: Control is also used as a synonym for safeguard or countermeasure

Employee Hand Book A documentation including instructions and information that employees shall abide or shall need to refer to in order to meet the terms and conditions of their employment

Guideline A description that clarifies what should be done and how, to achieve the objectives set out in policies

Information Processing Facilities Any information processing system, service or infrastructure, or the physical locations housing them

Information Security The preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved

Information Security Event An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

IRC Incident Reporting Contact is responsible for receiving and logging all reported IT incidents

IRT Incident Response Team is a group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations

IRTL Incident Response Team Leader

ISMS An Information Security Management System is a set of policies concerned with information security management.

KAU King Abdulaziz University

Mobile Code It is software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient

Service-Level Agreement (SLA) It is a negotiated agreement between two parties where one is the customer and the other is the service provider

Policy Overall intention and direction as formally expressed by management

Risk Combination of the probability of an event and its consequence

Risk Analysis A systematic use of information to identify sources and to estimate risk

Risk Assessment Overall process of risk analysis and risk evaluation

Risk Evaluation Process of comparing the estimated risk against given risk criteria to determine the significance of the risk

Risk Management Coordinated activities to direct and control an organization with regard to risk

NOTE: Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication

Risk Treatment Process of selection and implementation of measures to modify risk

Third Party That person or body that is recognized as being independent of the parties involved, as concerns the issue in question

Threat A potential cause of an unwanted incident, which may result in harm to system or organization

Vulnerability A weakness of an asset or group of assets that can be exploited by a threat