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

The information security policy is aimed to assure and communicate the management commitment and intent of supporting goals and principles for information security in line with KAU's business process.

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 Dean Role

- Enforce security policies within KAU environment to protect critical business information assets and software.
- Ensure that security policies are compliant with KAU legal and contractual requirement.
- Approve the use of all information systems used to process, store, or print sensitive information.
- Approve the new or modifications of existing security policies.

2. 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.

3. 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.

4. User Role

- Adhere to security policies, guidelines and procedures pertaining to the protection of sensitive data.
- Report actual or suspected vulnerabilities in the confidentiality, integrity or availability of sensitive data to Information Security Manager
- Use the information only for the purpose intended by KAU.

5. 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.

6. 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.

7. Related Policies

In accordance to best practices similar to ISO27001:2005 standard and mapped to its recommendations; the following policies were developed as part of a comprehensive information security program to support this Information Security Policy and the overall security posture of KAU:

- Risk Management Policy.
- Organizing Information Security Policy.
- Asset Management Policy.
- Personnel Security Policy.

- Physical and Environmental Security Policy.
- Communication and Operation Management Policy.
- Access Control Security Policy.
- Information System Acquisition and Development Policy.
- Information Incident Handling Security Policy.
- Business Continuity Planning Policy.
- Compliance Policy.

This document presents the information technology and information security policies entirely for KAU's information technology purpose. The document has been equipped with International information technology standards and best practices (ISO 27001 and COBIT). Additionally, KAU exercised acceptable level of professional due diligence and concentration to ensure quality and adequacy of information stated in this document.

8. Owner

- Information Security Manager.

9. Policy Statement

The information security policy is aimed to assure and communicate the management commitment and intent of supporting goals and principles for information security in line with KAU's business process.

Policy Objective	Policy Statement
Provide management directions and support for information security in accordance with business requirements and relevant laws and regulations [A.5.1]	➢ KAU shall commit to preserve the security of all the information assets owned and entrusted to them to ensure the legal and contractual conformity. KAU Management shall understand their responsibilities toward sustaining the information security objectives within the environment. ➢ International standards, globally accepted best practices, regulatory and legislative requirements shall be adopted in the KAU Information Security Management to guarantee: • Information is only accessed by authorized individuals, who have the proper and approved access authorization. • All the confidential information is well protected with all the necessary controls. • Information is only changed and/or updated only by authorized individuals who have the proper and approved authorization. • Information is always available to all the individuals who have the proper and approved authorization to access this information. • All Individuals who has been granted any form of access to information are fully accountable for the proper use of this information. ➢ A well structured information security framework based on the business

Policy Objective	Policy Statement
	requirements shall be defined and approved by the management. KAU Management shall commit to provide all the necessary support for the implementation of the information security framework. ➢ All KAU employees shall understand and acknowledge their responsibilities toward complying with the information security policies, procedures and standards. ➢ Information Security Department shall review and update Information security policies, procedures and standards on an annual basis. ➢ Information Security Department shall annually measure rhe effectiveness of the implemented controls in order to avoid security incidents and reduce resulting impacts, together with a process for benchmarking security maturity with other similar establishments. ➢ KAU Information security policies, associated standards and procedures shall be in compliance with legal, regulatory and international standards. ➢ Information Security Department in cooperation with the management shall ensure information security goals, objectives and its related activities are effectively achieve. ➢ All departments with the support of Information Security Department shall ensure their information assets have an acceptable level of security.

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