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 purpose of this policy is to establish a management framework to initiate and control the implementation of information security within KAU.

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. Administration Department Role

- Perform personnel screening.
- Issue general employment rules.
- Cooperate in user awareness and training.
- Cooperate with or Inform parties that are involved in case of changes of duties or employee termination.
- Conduct orientation and adaptation program of all new employees with regards to the organizational structure, roles and responsibilities.

6. 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.
- Risk Management Policy.
- Information Security Policy.

7. Owner

- Information Security Manager.

8. Policy Statement

Roles and responsibilities with respect to information security shall be defined throughout KAU to ensure proper security controls are implemented.

All the controls in this policy are in compliant with international best practices and standards (ISO27001).

1. Internal Organization

Policy Objective	Policy Statement
Manage information security within the organization [A.6.1]	➢ IT Dean shall define KAU information security goals and objectives. ➢ IT Dean shall provide direction and visible support for security initiatives. ➢ IT Dean shall clearly define a security management framework as well as the roles, responsibilities and qualifications of the people involved with security, resource management and security implementation. ➢ IT Dean shall develop and approve the information security policy, and ensure implementation tracking. ➢ Proper coordination between various departments shall be defined and established for relevant information security roles and job functions. ➢ Risk management methodologies covering the KAU business requirement and needs shall be defined and documented. ➢ Information security responsibilities shall be clearly defined and documented in accordance with the Information Security Organization Structure document. ➢ The assets and security processes associated with each particular system shall be identified and clearly documented. ➢ KAU shall define formal management authorization procedures for new information processing facilities.

Policy Objective	Policy Statement
	➢ Personal or privately owned information processing facilities shall not be permitted to be used within the organization without a written approval. ➢ Legal enforceable terms shall be considered in the confidentiality or non-disclosure agreements to address the requirement to protect KAU confidential information assets. ➢ Requirements relating to confidentiality and non-disclosure agreements shall be identified and re-examined on a regular basis. As such, the KAU shall: • Identify the information to be protected and required levels of sensitivity. • Indicate the expected length of the commitment. • Specify the terms for the return or destruction of information upon termination of the commitment. • Define the responsibilities and requirements with regards to signatories in order to prevent unauthorized dissemination of information. • Publish the penalties applicable in the event a user fails to respect the commitment. ➢ Information Security Department shall identify the relevant key external entities; and shall develop and maintain formal contacts with the identified relevant entities. ➢ KAU shall define adequate procedures that specify when and by whom authorities (e.g. law enforcement, fire department, supervisory authorities) shall be contacted, and how identified information security incidents shall be reported in a timely manner if it is suspected that laws may have been broken. ➢ Information security policies, procedures and technical standards shall be reviewed independently on a regular basis and in case of changing in the information security environment or documentations. ➢ The results of the independent review shall be recorded and reported to the management. These records shall be maintained.

2. External Parties

Policy Objective	Policy Statement
Maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties [A.6.2]	➢ All identified security requirements shall be addressed before providing external users to access to the KAU's information or assets. ➢ Where there is a need to allow an external party access to the information processing facilities, a risk assessment shall be carried out to identify any requirements for specific controls. ➢ Access by external parties to the KAU's information shall not be provided until the appropriate security controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. ➢ Accurate and updated record of external party's access to information processing facilities shall be maintained. ➢ Agreements with third parties involving accessing, processing, communicating or managing the KAU's information processing facilities shall cover all relevant security requirements.

Policy Objective	Policy Statement
	➢ KAU shall supervise third party access to KAU's information processing facilities.

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