Table of Contents

Issue Control....2
Change Approval....2
Review and Update....2
Policy Structure....3
1. Purpose....3
2. Scope....3
3. Role and Responsibilities....3
4. Compliance....4
5. Waiver Criteria....4
6. Related Policies....4
7. Owner....4
8. Policy Statement....5
Glossary....8

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 set the direction for establishing the responsibility, accountability and the management of KAU information assets that include information, software, hardware and people.

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. 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.

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.

إدارة الأصول
Asset Management

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.

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.
- Access Control Policy.
- Information Security Policy.
- Communications and Operations Management Policy.
- Information Security Incident Handling Policy.
- Information Systems Acquisitions, Development and Maintenance Policy.

7. Owner

- Information Security Manager.

Policy Statement

KAU Information systems, encompassing hardware and software, shall be managed in accordance with the information asset protection objectives established in the Asset Management Policy throughout the life cycle of the systems; from acquisition to disposal.

All Information systems, networks, and applications used in KAU production environment and in virtual premises, such as hosting sites, shall follow the documented change control process and procedures to ensure that only authorized updates or changes are made. Specific instructions and requirements for change control are as specified in the Communications and Operations Management Policy.

All production systems and applications developed by KAU or on behalf of KAU shall adhere to the documented process of analyzing, designing, developing, testing, and enhancing systems to ensure the integration of appropriate security controls.

1. Information Asset Inventory and Ownership

Policy Objective	Policy Statement
Achieve and maintain appropriate protection of organizational assets [A.7.1]	➢ KAU shall maintain an updated asset inventory of all the assets. ➢ KAU assets shall be categorized under the following main categories: • Hardware Assets • Software Assets • Information Assets • People Assets ➢ KAU shall keep an up-to-date inventory of their key configurations items (e.g., Application, Data, OS, DB, Patches, Hardware, etc). ➢ KAU shall identify an Information Asset 'Owner', who shall have the ultimate responsible for the information assets and all key decisions regarding the assets .Information asset owners shall collaborate to ensure definition of adequate controls for their information assets that provide a coherent and consistent level of protection. ➢ Ownership of assets shall be agreed and documented, assets. ➢ KAU shall consider the associated legal, regulatory and statutory requirements while deciding the protection level for information ➢ Protective security controls for information shall take into account classification and business needs for sharing or restricting information and the business impacts associated with such needs. ➢ The level of protection shall be assessed by analyzing confidentiality, integrity and availability and any other requirements for the information considered. ➢ For each asset the following shall be identified: • **Owners**: managers of organizational units that have primary responsibility for information assets associated with their functional authority. When owners are not clearly implied by

Policy Objective	Policy Statement
	organizational design, the IT Manager shall make the designation. Owners are responsible for: ▪ Identification of information assets. ▪ Assigning the proper information asset classification. ▪ Ensuring the proper labelling whenever is applicable for sensitive information. ▪ Designating the custodian in possession of the information. ▪ Ensuring the information classifications are properly communicated and understood by the custodians. ▪ Reviewing information assets classification. • **Custodians**: managers, administrators, service providers, and those designated by the owner to manage, process, or store information assets. Custodians are responsible for understanding the information classifications, and applying the necessary controls to maintain and conserve the information classifications and labelling established by the Owners. • **Users**: individuals, groups, or organizations authorized by the Owner to access information assets. Users are responsible for: ▪ Understanding the information classifications, abiding by the controls defined by the owner and implemented by custodians ▪ Maintaining and conserving the information classification and labelling established by the Owners. ▪ Contacting the Owner when information is unmarked or the classification is unknown. ➢ KAU shall define and document an Acceptable Use Policy that defines the guidelines for Asset management. ➢ All the assets shall be only used for business purposes in serving the interests of KAU in the course of normal operations. ➢ KAU shall audit and monitor network and system activities on a periodic basis to ensure compliance with this policy. The governing body shall periodically review the access rights and security practices with relation to use of computing resources. Any violation of network and system use shall be reported to respective KAU management in a timely fashion. ➢ Users shall be responsible for exercising good judgment regarding the reasonableness of personal use. ➢ All employees, contractors and third party users shall follow rules for the acceptable use of information and assets associated with information processing facilities, including: • Rules for electronic mail and Internet usages. • Guidelines for the use of mobile devices, especially for the use outside the premises of the organization. ➢ All users shall not participate in illegal activities such as accessing unauthorized assets, hacking, introducing any computer contaminant or computer virus, committing acts, which may disrupt use of the assets.

2. Information Asset Classification

Policy Objective	Policy Statement
Ensure that information receives an appropriate level of protection [A.7.2]	➢ All information assets shall be classified into one of the following four categories based on their sensitivity, privacy requirements, and value to KAU: • Secret • Confidential • Internal Use • Public ➢ When information of various classifications is combined, the resulting collection of information or new information shall be classified at the most restrictive level among the sources. ➢ Classification of information shall be reviewed by the Information Owner in a periodic basis, with the change in sensitivity. ➢ KAU shall develop classification guidelines and scheme that include conventions for initial classification and reclassification over time; in accordance with predetermined access control policy. ➢ All KAU information assets shall be labelled as on the basis of sensitivity and KAU assets management policy. Appropriated asset handling scheme for labels shall be adopted by the management. ➢ Documents, hardware items and removable media physical labelling shall include appropriate security classifications in accordance with KAU's assets management. ➢ Procedures for handling and storage of information shall be established in order to protect such information from unauthorized disclosure or misuse. ➢ All users shall follow a formal authorization process before making any proprietary information, publicly available. The integrity of such information shall be protected after making it public also.

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