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 ensure that KAU's security is integrated and implemented throughout the whole lifecycle of information systems acquisitions, development and maintenance.

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.

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.
- Asset Management Policy.
- Communications and Operations Management Policy.

7. Owner

- Information Security Manager.

8. Policy Statement

Information security in KAU shall be addressed throughout the developing or/and acquisition process of new information systems.

1. Security Requirements Analysis and Specification

Policy Objective	Policy Statement
Ensure that security is an integral part of information systems [A.12.1]	➢ Security requirements for new information systems or enhancements to existing information systems shall be analyzed and necessary controls shall be introduced through a formal process. ➢ KAU shall ensure that information system development or acquisition activities are performed according to the documented requirements, standards and procedures. ➢ KAU shall ensure to define, document, implement and monitor system specific risk based information security controls for all key systems supporting its operations. ➢ IT Deanship with support from Information Security Department and Information Asset Owner shall be responsible to execute the defined

Policy Objective	Policy Statement
	process. ➢ KAU shall conduct a Security Threat and Risk Assessment during the requirements phase when developing, implementing major changes to, or acquiring an information system to: • Identify the necessary security requirements to safeguard the information system. • Assign information and information system security classification. ➢ KAU shall ensure that sufficient controls are in place to mitigate the risk of information loss, error or misuse from information systems. ➢ KAU shall ensure that a system security plan is adequately documented and maintained for each information system.

2. Processing Applications

Policy Objective	Policy Statement
Prevent errors, loss, unauthorized modification or misuse of information in applications [A.12.2]	➢ Appropriate validation checks shall be applied to applications and database systems in order to validate input and output data. In the case of sensitive data, additional controls shall be incorporated as required. ➢ Processing controls shall be designed into applications and database systems to detect corruption of information whether resulting from processing errors or deliberate acts. ➢ Integrity controls shall be designed into applications to ensure authenticity and protect message integrity within applications. ➢ Output controls shall be designed into applications to validate the correct and appropriate processing of stored information. ➢ Changes to documents and sources of input data shall be authorized. ➢ Responsibilities of all staff involved in data input or output processes shall be defined and documented. ➢ When an application takes inputs from file uploads, necessary validations shall be conducted on relevance of file type and size. ➢ A mechanism for fault logging and criteria shall be defined for handling the reported faults. The environment shall be constantly monitored for any adverse event.

3. Cryptographic Controls

Policy Objective	Policy Statement
Protect the confidentiality, authenticity or integrity of information by	➢ Encryption controls shall be implemented as required on critical business applications accessible over Internet or any systems that might have sensitive information.

Policy Objective	Policy Statement
cryptographic means [A.12.3]	➢ Data transferred through Internets shall be adequately protected with suitable encryption technologies. ➢ A secured method shall be adopted for Key Management while using encryption methodologies in the enterprise. ➢ Import, export and use of encryption methodologies shall be in compliance with applicable laws and regulations. ➢ Digital certificates based on Public Key Infrastructure (PKI) shall be implemented for identified critical applications in the enterprise based on the business requirements. ➢ Users shall exercise caution for signing, encryption or signing and encrypting messages depending on the sensitivity of messages in the KAU.

4. Systems Files Control

Policy Objective	Policy Statement
Ensure the security of systems files [A.12.4]	➢ Procedures shall be implemented to control the installation of software on operational systems, and to minimize the risk of interruptions in or corruption of information services. ➢ All information systems shall be securely hardened through secure configuration in accordance with International Best Practice Standards. ➢ End-point security controls shall be implemented to restrict the use of system devices and peripherals. ➢ KAU administrators shall be only the authorized personnel to perform updates to the operational software, applications, and program libraries. ➢ Information system in development shall be never running in an operational environment. ➢ KAU shall ensure that formal configuration procedures are adequately documented and maintained. ➢ Any decision to upgrade to a new release shall consider KAU business and security requirements. ➢ Operation procedures for systems shall be clearly documented and an activity log detailing the all types of activity shall be maintained. This activity log shall be monitored periodically in compliance with KAU policies and procedures. ➢ KAU shall ensure that all source codes are compiled, controlled and maintained centrally. ➢ Access to program source codes and configurations shall be documented and restricted to authorized personal.

5. Development and Support Processes Security

Policy Objective	Policy Statement

Policy Objective	Policy Statement
Maintain the security of application system software and information [A.12.5]	➢ KAU shall ensure that a formal change control procedures is adequately documented and enforced. ➢ All changes or installation of new software shall be tested in a test environment. ➢ Production environment shall be isolated from testing and development environment. ➢ KAU shall ensure that all changes to information systems are accurately tested, recorded, updated and maintained. ➢ Implementation of changes shall takes place at appropriate time and it shall not effect negatively on the business process of KAU. ➢ Security measures shall be taken to minimize the risk of information leakage from equipment processing sensitive information. Protection measures shall be in accordance with the Asset Management Policy. ➢ System capacity requirements shall be planned before introduction of a new critical business application and reviewed during upgrades. Due precautions shall be take to avoid any availability issues of existing applications or systems. ➢ Acceptance criteria shall be clearly defined for upgrades of systems and new versions. ➢ Acceptance tests shall be planned and carried out as per the plan. ➢ Documenting of change management and impact analysis on an ongoing basis for application changes shall be part of the system development life cycle.

6. Managing Technical Vulnerability

Policy Objective	Policy Statement
Reduce risks resulting from exploitation of published technical vulnerabilities [A.12.6]	➢ KAU shall take proactive steps to identify and minimize the vulnerabilities in its technology environments before it can be exploited. ➢ Information Security Department shall be responsible to take necessary steps to provide security of KAU infrastructure. ➢ Any new patches shall not be installed in production environment unless they are properly tested and evaluated in test environment. ➢ Personnel who are performing vulnerability management duties shall ensure the following: • Security scanning tools shall be used on a prescribed basis to identify vulnerabilities that could be exploited by persons performing unauthorized scanning with similar tools. • Multiple tools with different technologies shall be used to identify as much vulnerability as possible. • Both Internet and Intranet-facing assets shall be scanned. • The Information Owner shall be notified of and accept potential effects of the scanning activity on the target environment before

Policy Objective	Policy Statement
	scanning is initiated. • Third party sources of technical vulnerability information (e.g., security alerts, system patches, workarounds, and virus updates) shall be monitored for KAU-relevance. As vulnerabilities are reported by these third party sources, personnel performing vulnerability management duties shall compare each vulnerability to their inventory to determine whether their IT resources are susceptible. • If a vendor releases a patch to repair a security related control, the patch release shall be considered an implicit vulnerability notification and risk mitigation shall be taken. • All approved devices attached to a State network and running operating systems and applications with identified security vulnerabilities are patched so as to address known vulnerabilities. • If a device attached to a network cannot be patched, the vulnerability is mitigated with an acceptable alternate security control.

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