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 develop a framework for timely and effective handling of information security incidents. An information security incident is a suspected or confirmed violation of the integrity, availability or confidentiality of the corporate information that shall cause or has affected the organisation's security.

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. Legal Department Role

- Ensure that the Information Security Policies is compliant with the existing legal and contractual requirement.
- Provide the expert legal advice necessary for the other departments to provide services in a manner that fully compliant with existing laws and regulations.
- Take action as far as the prosecution of the suspect is concerned.

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

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

1. Reporting Information Security Incidents

Policy Objective	Policy Statement
Ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken [A.13.1]	➢ Security and potential security incidents shall be communicated to relevant personnel who will assist in corrective actions to be taken. ➢ All suspected security incidents shall be reported immediately to the Incident Response Team- IRT. ➢ KAU shall develop a proper procedure with descriptive steps about information security incident handling. ➢ All KAU staff shall understand their responsibility towards reporting security incidents that have known or potential impact on information security.

2. Managing Information Security Incidents

Policy Objective	Policy Statement
Ensure a consistent and effective approach is applied to the management of information security [A.13.2]	➢ Information Security Department shall develop and implement appropriate procedures for performing routine incident detection activities, reporting security incidents, control and repair damage and prevent future damage to the KAU resources. ➢ Incident Response Team-IRT shall decide when events are classified as an incident and determine the most appropriate response. ➢ Only identified and authorized staff shall have access to the affected systems during the incident and all of the remedial actions shall be documented in as much detail as possible. ➢ Information security events and weaknesses shall be reported to a nominated central point of contact within Incident Response Team-IRT as quickly as possible and the incident response and escalation procedure shall be followed. ➢ The central point of contact is responsible for coordinating all efforts to manage and resolve related incidents. The person shall form an incident response team (IR Team) and shall lead the team members and other KAU employees to contain the damage caused by the incident and resolve incident. ➢ The central point of contact shall record the incident and allocate an incident number for tracking and future reference. ➢ The central point of contact shall be responsible to keep a track of status of incident by following up with relevant persons and handling queries related to status of incident ➢ The central point of contact may further escalate the incident to higher levels of KAU management depending on the severity or impact of an incident. ➢ The central point of contact shall analyze the incidents based on the data received from the incident reporter and shall seek more information from the reporter if required.

Policy Objective	Policy Statement
	➢ The reporting procedure shall be quick and have redundancy built in. ➢ An escalation procedure shall be incorporated into the response process so that users and support staff are aware who else to report the event to if there is no response within a defined period. ➢ Based on data available and level of criticality of incident, the Information Security Department shall send out incident alerts to departments which could possibly be affected by similar incidents. ➢ Once the full recovery from the Incident has been done an additional monitoring means shall be implemented for a specific duration to ensure the incident has been fully treated. ➢ KAU shall conduct thorough investigations into the root cause of each security incident and take appropriate action to: • Warning, discipline or prosecute those responsible. • Update existing security controls or introduce new ones to prevent a recurrence of the same incident. • Update a register of security incidents for accurate reporting. ➢ Information Security Department shall regularly review and update incident response plans and procedures. ➢ KAU shall adopt effective mechanisms to measure incidents and its impacts. Based on the information gained from the incident, Information Security Department shall make necessary changes (if required) to security policies; enhance controls where applicable to limit the frequency of occurrence, damages and cost. ➢ Incident Response Team-IRT customizes the relevant pre-existing plan(s) to finalize a corrective action plan specific to the incident to the extent possible within the available timeframe ➢ The actions required to recover from the security incident shall be under formal control. ➢ Information Security Department and IT Deanship shall identify, document, and maintain rules for collection, retention and presentation of evidence laid down in the relevant jurisdictions. ➢ If an incident may require information to be collected for an investigation strict rules shall be adhered to. The collection of evidence for a potential investigation shall be approached with care. ➢ Information Security Department and Information Technology, Department and shall be contacted immediately for guidance and investigation; and strict processes shall be followed for the collection of forensic evidence. ➢ Incident evidences shall be collected, secured and preserved properly, because such materials are evidence of the discovery of any breach. ➢ KAU shall have a documented incident response program and plan in place covering major types of incidents. Every incident response plan shall be tested for effectiveness through appropriate means such as simulation exercises. ➢ Information Security Department shall maintain a detailed documentation specifying the history of incidents. ➢ Information Security Department shall regularly gather and review the post incident 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