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

Access control policy of KAU is to manage logical and physical access only to authorized individuals and devices inside the KAU premises.

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 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.

3. 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.

4. 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.

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.

6. Legal Department Role

- Ensure that the Information Security Policies are 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.
- Information Security Policy.
- Information Security Incident Handling Policy.

7. Owner

- Information Security Manager.

8. Policy Statement

KAU shall establish a formal process for hiring, resigning and terminating of all employees. KAU shall identify and deliver security awareness for all employees as a part of staff induction program.

1. Prior to Employment

Policy Objective	Policy Statement
Ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and reduce the risk of theft or misuse of facilities [A.8.1]	➢ All employees shall be responsible towards protecting all assets owned and /or entrusted to KAU. ➢ All employees shall be responsible towards reporting to their direct managers any existing or potential attacks or threats within KAU's environment. ➢ Department managers shall be responsible to identify the skill sets needed for the proper operation of the personnel within their departments. ➢ Department managers, in coordination with the Administration Department, shall ensure that all employee's recruitment processes are complaint with KAU's policies and procedures. ➢ Appropriate background verification checks "screening" for all candidates for employment, contractor status, or third party user status, shall be carried out by Administration Department or appropriate third parties. ➢ Where the staff is provided through an agency, the contract shall specify the Agency's responsibilities towards personnel background checks. ➢ Administration Department shall prepare proper induction material to be provided to the newly employed personnel as guidance for the positions they are required to fulfill the controls and specific measures undertaken for any of those positions. ➢ All employees shall commit and admit in writing that they have read, understood and accepted KAU's Information Security Policy. ➢ Information security responsibilities needed to be abided by all employees and it shall be incorporated into KAU Employee Handbook. ➢ Specific information security responsibility shall be incorporated into all contracts with contractors (including consultants or any non-employee who performs work-for-hire) who will have access to restricted, customer or

Policy Objective	Policy Statement
	otherwise sensitive information. ➢ Administration Department in coordination with department managers shall document the roles and responsibilities in the job definition as applicable as in the Information Security Policy. ➢ Job definition shall include any specific responsibility towards security, as applicable to a role. ➢ Mangers shall be aware of the personal circumstances of their staff and shall be on the lookout for any behavioural change that may lead to security breach. ➢ The terms and condition of employment shall specifically mention the responsibility of the employee towards security through Confidentiality Agreement. ➢ All employees, contractors and third party users of KAU shall sign the terms and conditions of employment/engagement as an indication of acceptance. ➢ All staff shall sign an appropriate Confidentiality or Non-Disclosure agreement at the time of joining. In addition to KAU own policies, procedures, standards and guidelines. ➢ Contract staff or contract agency providing staff visiting sensitive areas shall be required to sign a Confidentiality Agreement as required.

2. During Employment

Policy Objective	Policy Statement
Ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and reduce the risk of human errors [A.8.2]	➢ All employees, and, where relevant, contractors and third party users, shall receive appropriate awareness training and regular updates of organizational policies and procedures relevant to their job functions. ➢ KAU shall ensure that all personnel are aware of information security requirements; and shall be trained on the security requirement and processes associated with their jobs. ➢ All personnel shall receive refresher training on KAU information security requirements at least once a year. ➢ Formal disciplinary process shall be followed for employees violating or persistently breaching the security policies, in order to prevent further violations by others. ➢ The disciplinary process shall ensure correct and fair treatment for employees who are suspected of committing security breach. ➢ KAU shall take an adequate precaution to segregate employee duties in order to reduce opportunities for unauthorized modification or misuse of information. ➢ Information processing facilities shall not be used for purposes other than business. Any such fraudulent activities detected shall be dealt as per disciplinary action procedure. ➢ All employees and contractors shall understand the responsibility of reporting any security or potential events or other security risks to the KAU. ➢ Administration Department shall ensure that all reported fraudulent activities are investigated.

3. Termination or Change Employment

Policy Objective	Policy Statement
Ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner [A.8.3]	➢ KAU shall clearly define and assign responsibilities and practices for performing employment termination or change of employment. ➢ All employees, contractors and third parties shall return the entire KAU's information and physical assets in their possession upon termination of the employment or contract. ➢ Access rights to information and information processing facilities shall be removed upon termination of the employment or contractual agreement. ➢ The Administration Department in cooperation with the relevant Departments shall, if necessary, ensure that employees, who hold key positions and have given notice of their intention to leave KAU, shall be transferred to positions from which they can cause minimum harm to KAU's information assets. Alternatively, it is up to their manager to give them mandatory leave.

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