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 compliance policy is to provide KAU employees with the necessary requirements to avoid any breaches of the information security policies, laws, regulatory, contractual obligations and any security requirements.

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. 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

- All information Security Policies.

7. Owner

- Information Security Manager.

8. Policy Statement

All the necessary controls shall be defined to ensure that all employees, contractors and consultants comply with KAU laid down information security policies, laws, regulatory or contractual obligations, and any security requirements.

1. Legal Requirements

Policy Objective	Policy Statement
Avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements [A.15.1]	➢ KAU shall identify and analyze external regulatory requirements for their impact on its IT function, and take appropriate measures to comply with them. ➢ KAU shall identify and document all the relevant statutory, regulatory and contractual requirements. ➢ KAU shall ensure that the design and operation, of information systems and related facilities are complaint with all applicable legal, regulatory or contractual security requirements ➢ Statutory, regulatory and contractual requirements related to systems shall be documented within the system security manuals. ➢ A management structure and security control shall be defined to ensure

Policy Objective	Policy Statement
	compliance with this policy and all relevant data protection laws and regulations required as per KAU requirements. ➢ Personal information shall not be transferred or shared when statistical information could be used as an alternative. ➢ Records classification and protection procedures shall be defined and documented to protect records from misuse, loss, destruction and falsification. ➢ KAU shall understand the importance of intellectual property rights associated with its information systems. Intellectual property may include, but not limited to: • Software • Document copyright • Design rights • Trademarks • Patents • Source code licenses ➢ KAU Intellectual Property Rights shall be defined as: • Deliverables created by KAU internally without an external sponsor customer. • Deliverables created jointly by KAU and third party where parties agree under a contract (Written Understanding) that Intellectual Property Rights would belong to KAU. ➢ KAU shall comply with: • Copyright requirements associated with proprietary material, software, and designs acquired by KAU. • Licensing requirements limiting the usage of products, software, designs and other material acquired by KAU. ➢ KAU shall develop and implement proper procedures for ensuring that legislations, regulations and contractual requirements are complaint with intellectual property rights. ➢ Compliance with product copyright and licensing requirement shall be maintained and regularly check. ➢ KAU shall maintain and protect its own evidence of licenses or manuals ownership. ➢ KAU shall adopt a documented policy that defines the appropriate approach for disposing or transferring software to others. ➢ Physical and logical access to joint materials (between KAU and third party) shall be only granted and controlled based on “need to know” and “need to access” principles. ➢ Software copyrights shall be protected as per the terms of contract and appropriate awareness shall be conducted amongst users. ➢ KAU shall implement appropriate security controls to prevent materials and software of KAU Intellectual Property Rights form any form of unauthorized misuse.

Policy Objective	Policy Statement
	➢ KAU shall not duplicate third party materials, convert them to another format or extract them from commercial recordings (film, audio) other than permitted by copyright policy. ➢ All users shall acknowledge that their misuse of the materials may result in the violation of Intellectual Property Rights of third parties. ➢ KAU shall define and document an appropriate Information processing facilities acceptable use policy. ➢ All users shall be aware of the well defined scope of their authorized access and of the monitoring in place to detect unauthorized use. ➢ All users shall acknowledge that their misuse of information processing facilities may result in the breach of confidentiality with relation to KAU obligations, and they are bounded by the KAU policies.

2. Information Security Policies, Standards and Technical

Policy Objective	Policy Statement
Ensure compliance of systems with organizational security policies and standards [A.15.2]	➢ Each department shall ensure that their associated policies, procedures and standards are fully compliant with KAU Information Security Policies and Standards. ➢ All users shall understand and acknowledge the responsibility towards complying with KAU Information Security Policies and Standards. ➢ KAU shall conduct an appropriate technical compliance evaluation twice a year. The evaluation may include, but not limited to: • Examination of operational systems. • Penetration testing. • Vulnerability assessments. ➢ Penetration testing and vulnerability assessments shall be carried out whenever possible to assess the effectiveness of the implemented controls. ➢ A technical compliance checking shall only be carried out by competent, authorized persons, or under the supervision of such persons.

3. Information Systems Audit

Policy Objective	Policy Statement
Maximize the effectiveness of and minimize interference to/from the information systems audit [A.15.3]	➢ All audits shall be individually tracked for closures and any significant audit exceptions shall be reported to the respective department head as well as to the management. ➢ Audit finds for both planned and unplanned audits shall be based on the type of risks (e.g. critical risk, high risk, medium risk, low risk or very low risk). Auditors shall classify the findings as Non-compliance to the documented procedure or inadequacy in the system.

Policy Objective	Policy Statement
	➢ KAU shall restrict and control the usage of systems audit tools in accordance with specific guidelines for this purpose. ➢ Information systems audit tools, e.g. software or data files, shall be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

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