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

In order to maintain, the confidentiality, integrity and availability of KAU's information assets transmitted over the communication networks and the proper operation of those assets, KAU shall deploy all necessary communications/network and operational controls.

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. Information Security 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.

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.
- Access Control Policy.
- Asset Management Policy.
- Information Security Incident Handling Policy.

7. Owner

- Information Security Manager.

8. Policy Statement

Communications and operations management is an important function that has a significant impact on information security. Due to the level of access to the information systems available at this level, detailed documented operating procedures, including an appropriate level of segregation of duties is required.

All KAU's communications equipment including computer systems and network devices shall be protected to ensure the confidentiality, integrity and availability of information processing facilities.

1. Operational Procedures

Policy Objective	Policy Statement
Ensure the correct and secure operation of information processing facilities [A.10.1]	➢ KAU shall establish and develop processes, procedures, standards and guidelines based on KAU operational requirements. ➢ KAU shall implement appropriate technical countermeasures and technologies to protect the confidentiality and integrity of KAU's sensitive information and systems while travelling through untrusted networks. ➢ All the necessary changes to KAU assets shall follow the KAU documented change management procedure. ➢ Any type of change shall be tested and applied in the test environment prior to authorize the implementation of the change in the production environment. ➢ Implementing, transferring newly developed or updated software from development to production environment shall follow a well documented procedure for that purpose. ➢ KAU shall implement segregation of duties principle, where appropriate, to reduce the risk of negligent or deliberate system misuse. ➢ In KAU, where segregation of duties is not applicable, other controls shall be in place to compensate e.g. monitoring of activities, maintenance and review of audit trails. ➢ No live data shall be used to perform testing to any systems, neither in production nor in test environment.

Policy Objective	Policy Statement
	➢ KAU shall develop and prepare appropriate documented procedures for system activities associated with information processing and communication facilities.

2. Managing Third Party Service Delivery

Policy Objective	Policy Statement
Implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements [A.10.2]	➢ KAU shall only provide third party access to facilities and data which are required to perform specific agreed tasks. ➢ KAU shall only provide the third party access after the third party has signed a non-disclosure agreement. Non-disclosure agreement executed between KAU and third party shall be in accordance with KAU legal compliance policy. ➢ IT Deanship staff shall update their list of contracts, outsourced services as well as SLA targets and their corresponding contact details. ➢ KAU shall assign a designated individual or service management team for managing the relationship with a third party. ➢ KAU shall maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a third party. ➢ KAU shall follow a formal process to connect information assets with the third party. ➢ KAU shall randomly perform an audit on third party access for security violations, improper use, and assessment of need. ➢ KAU shall regularly monitor and review the services, reports and records provided by the third party. ➢ Any documents created by third party related to business engagement with KAU shall be classified by third party depending on the sensitivity of the document and as per the information classification policy of KAU. ➢ Third party staff working for KAU shall have proper understanding and awareness of KAU Information Security Policy.

3. System Planning

Policy Objective	Policy Statement
Minimize the risk of systems failures [A.10.3]	➢ KAU shall address new systems performance and capacity requirements in the planning and acceptance phase. ➢ Acceptance criteria shall address the vendor guarantee that installation of the new system shall not negatively affect the existing systems. ➢ KAU shall identify capacity requirements for all new and ongoing activities. ➢ The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

Policy Objective	Policy Statement
	➢ KAU shall ensure that the requirements and criteria for acceptances of new systems are clearly defined, agreed, documented and tested. ➢ New information systems, upgrades, and new versions shall only be migrated into production after obtaining formal acceptance. ➢ For major new developments, KAU shall consult the operations function and users during the development process to ensure the operational efficiency of the proposed development. Appropriate tests and checks shall be carried out to confirm that all acceptance criteria have been fully satisfied.

4. Controls against Malicious and Mobile Code

Policy Objective	Policy Statement
Protect the integrity of software and information [A.10.4]	➢ KAU shall define and implement a proper mechanism to prevent, detect Malicious Code and resolve the infected systems in a proper and timely manner. ➢ Centralized antivirus software shall be implemented at various levels in the network and system infrastructure as part of a layered approach to reduce Malicious Code entry into KAU environment. ➢ The centralized antivirus server shall automatically update virus signatures from the service provider, and whenever there is a new update of signature or virus engine is available. ➢ All possible and practical measures shall be taken to prevent the introduction of Malicious Code into KAU information systems and network. ➢ The anti- Malicious Code software shall be configured to automatically scan all removable media drives and flash memories when they are connected. ➢ KAU shall define and implement appropriate procedures to regularly collect information, such as subscribing to mailing lists and/or checking web sites giving information about new malicious code. ➢ KAU shall prevent any installation of unauthorized or illegal software on any information systems. ➢ KAU shall effectively protect and prevent users from changing, removing, disabling or tampering with the Malicious Code prevention/detection software that has been installed on their machine. ➢ Users shall understand their responsibility to report any issues related to suspected presence of Malicious Code (if any) to Information Technology Department. ➢ All exchanged media between various departments or organizations shall be properly checked against Malicious Code prior using and sharing it. ➢ Malicious Code protection software shall be configured to perform automatic scan periodically on all PC's, servers, laptop computers and other components of KAU information systems architecture to detect potential Malicious Code. ➢ System Administrator shall monitor antivirus software in a regular basis so

Policy Objective	Policy Statement
	to ensure that any virus incidents are quickly dealt with.

5. Information Backup

Policy Objective	Policy Statement
Maintain the integrity and availability of information and information processing facilities [A.10.5]	➢ Information Security Department through close interaction and coordination with the System and Data Owners shall identify Backup and restoration requirements of all KAU systems in line with legal and regulatory implications, vendor recommendations and other relevant factors. ➢ All application and operating systems software, data (including databases), user configuration information and hardware configuration information (where applicable) shall be backed up in accordance with the procedures recommended by vendor/implementer. ➢ Restoration of backups will require specific and appropriate authorization and shall be performed in accordance with the Backup and Restoration Procedure. ➢ Backed up data shall be checked and tested regularly to ensure that its integrity and effectiveness through restoration of selective data. ➢ The backup media shall be appropriately labeled and numbered automatically by the backup system or manually by the System Administrator taking the backup. ➢ Reliable agency shall be used for transporting backup media to identified off-site location. In such cases, courier agency shall sign a Non-Disclosure agreement with KAU; and sealed envelopes with signature shall be used. ➢ The backup logs shall be maintained and kept up-to-date; and shall be in the form of hard copies. ➢ Backup logs shall be reviewed by the respective System Administrator to ensure proper backup. ➢ Wherever possible, backup that contain sensitive information shall be encrypted. ➢ Appropriate backup media shall be chosen by System Administrator based on the criticality of data and retention period. ➢ System Administrator shall understand the responsibility to report any condition that might result in the loss of backup data integrity, confidentiality or availability for any reason.

6. Managing Network Security

Policy Objective	Policy Statement
Ensure the protection of information in networks	➢ KAU shall identify and implement appropriate countermeasures to:

Policy Objective	Policy Statement
and the protection of the supporting infrastructure[A.10.6]	• Safeguard the confidentiality and integrity of data passing over public networks or over wireless networks. • Protect the connected systems and applications. • Maintain the availability of the network services and computers connected. ➢ Network operation responsibility shall be separated from the computer operation responsibility to avoid interference. ➢ Logging and monitoring of network activities shall be applied to enable recording of any security actions. ➢ KAU shall protect Information Technology infrastructure by implementing proper network security measures and features. ➢ Network services agreement shall be defined for network services provided in-house or through third parties and shall include security features, management requirements and service levels.

7. Managing Media

Policy Objective	Policy Statement
Prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities [A.10.7]	➢ Information asset owners shall ensure that the media is managed and controlled in accordance with applicable KAU policies and procedures. ➢ All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications. ➢ Information stored on media that needs to be available longer than the media lifetime (in accordance with manufacturers' specifications) shall be stored elsewhere to prevent information loss due to media degradation. ➢ Personal information shall be kept on removable media when it is absolutely necessary to do so; and shall be encrypted. ➢ Removable media drives shall only be enabled if there is a business reason for doing so. ➢ All removable media shall be registered in an updated log to limit the opportunity for data loss. ➢ Removable re-writable media that is not in use any more should be re-initialized to prevent unintended information disclosure during exchanges amongst employees or other parties. ➢ All media shall be disposed as per the Information Classification, Labelling and Handling Procedure, Retention period or end of use of media. ➢ All disposed media shall be logged in an updated media disposal login order to maintain an audit trail. ➢ The physical media shall be protected and controlled while in transit by deploying proper security controls. ➢ Proper logging and tracking of each physical media in transit shall be exercised by the exchanging parties; the receiving party shall notify the sending party of the receipt of the physical media in good standing

Policy Objective	Policy Statement
	condition. ➢ Media being transported shall be protected from unauthorized access, misuse or corruption.

8. Information Exchange Procedures

Policy Objective	Policy Statement
Maintain the security of information and software exchanged within an organization and with any external entity [A.10.8]	➢ KAU shall protect and control exchange of critical business information assets and software in order to prevent loss, modification, destruction, or misuse of information. ➢ Information owners shall ensure appropriate mechanisms are in place to protect exchange of information. ➢ Formal agreements shall be established for the exchange of critical business information assets or software with external entity. ➢ Prior to the exchange of information assets with external entity a formal agreement shall be defined. ➢ Wherever possible cryptographic techniques shall be adopted and implemented to protect the confidentiality, integrity and authenticity of sensitive information. ➢ KAU's sensitive or critical information shall not be left on copiers, printers, and facsimile machines, as these could be accessed by unauthorized personnel. ➢ A formal policies, procedures, and standards shall be established and maintained to protect media transportation beyond KAU premises against unauthorized access, misuse or corruption. ➢ Use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood internally and that the information is appropriately protected. ➢ An appropriate, well understood and agreed on labeling system shall be used in KAU. ➢ Security controls shall be established to protect electronic messaging (E-mail) from unauthorized access, modifications or denial of service. ➢ Third party from which KAU receives sensitive data may have their own policies regarding the handling and processing of such data. Users shall ensure that they comply with the relevant policies before handling or processing data belonging to such third party. ➢ All users shall manage the creation, storage, amendment, copying and deletion or destruction of data (in electronic and paper form) in a manner which is consistent with the KAU policy, and which controls and protects the confidentiality, integrity and availability of such data.

9. Electronic Commerce Services

Policy Objective	Policy Statement
Ensure the security of electronic commerce services, and their secure use [A.10.9]	➢ All information related to electronic commerce passing over public networks shall be protected from any dispute, fraudulent activity, and unauthorized disclosure and modification. ➢ All information related to on-line transactions shall be protected from miss-routing, incomplete transmission, unauthorized disclosure, unauthorized message alteration, unauthorized message duplication or replay. ➢ All publicly available systems shall be protected from unauthorized modification.

10. Monitoring Information Processing Activities

Policy Objective	Policy Statement
Detect unauthorized information processing activities [A.10.10]	➢ Based on the criticality of the data, Information Security Department shall ensure that specific and adequate levels of audit trails are implemented; and shall be enabled in the applications and databases. ➢ Information Security Department shall ensure that detailed audit trails of user account creation, deletion and revocation of access rights are recorded and kept for a minimum of 5 years. ➢ All system transaction services shall log user account information and digitally sign such logs in order to prevent repudiation of user transactions. ➢ KAU shall ensure that information security controls in place, are affective, and are not being bypassed. ➢ KAU shall ensure that all detected bad behaviour and vulnerability exploitation are monitored and logged. Where possible a security baseline shall be developed. ➢ KAU shall ensure that all system administrators do not have permission to modify or de-activate logs of their own activities. ➢ KAU shall ensure that the date and time stamp of the audit trails for all online system components are synchronized to facilitate the tracking of user's identity and online activities. ➢ All server and network device clocks shall be synchronized to ensure accuracy of security log file data. ➢ KAU shall review the results of monitoring activities according to the risks involved.

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