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 KAU business continuity policy is to define appropriate actions to mitigate any interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

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. 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.

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.
- Risk Management Policy.
- Asset Management Policy.
- Information Security Incident Handling Policy.

7.Owner

- Information Security Manager.

8. Policy Statement

KAU business continuity planning shall include controls to identify and reduce risks, to contain the damaging incidents and to ensure that information required for business processes is readily available within KAU.

1. Business Continuity Management

Policy Objective	Policy Statement
Counteract interruptions to business activities and protect critical business process from the effects of major failures of information systems or disasters and ensure their timely resumption [A.14.1]	➢ Information security requirements shall be taken into considerations while planning and developing the Business Continuity Management. The following are some of the key elements: • Developing a Formal Business continuity strategy. • Developing a Framework for the Business Continuity Planning. • Conducting Business Impact Analysis and Risk Management. • Developing and Implementing Business Continuity Plans. • Developing and Implementing Disaster Recovery and Resumption Plan. • Maintaining and Re-Assessing Business Continuity Plans. • Testing Business Continuity Plans. ➢ The Business Continuity Department shall conduct a bi-annual BIA to identify and prioritize the critical business processes and costs of downtime. The BIA shall cover the major business processes that cut across multiple business units or organizations. It shall identify the business process availability Recovery Time Objectives (RTOs) and business process Recovery Point Objectives (RPOs). ➢ The Information Security Department shall extend the results of the BIA to the business units as a basis for developing business unit-specific BIAs, identifying key business processes and the associated risks if these processes were not available. Each business unit shall appoint a Business Continuity Coordinator who will coordinate the development of the business unit-specific BIAs and resulting business unit-specific BCP, with guidance of the Business Continuity Department. ➢ Business Continuity Plan shall be developed, using the results from the risk assessment, which will determine the overall approach to business continuity. ➢ The risk assessment shall identify, quantify, and prioritize risks based on KAU business requirements and goals relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities. ➢ Business Continuity Plans shall be implemented to reduce the impact from the loss of information assets to an acceptable level, through a combination of preventive and recovery controls. Business Continuity Planning shall be based on identified risks that can cause interruptions to business processes (e.g. equipment failure, fire, etc) and an impact analysis to determine the probability and impact of such interruptions in terms of time, damage scale and recovery period. ➢ Risks that can cause interruptions to business processes (e.g. equipment failure, fire, human errors, theft, etc) shall be identified, along with the

Policy Objective	Policy Statement
	probability and impact of such interruptions and their consequences. ➢ As part of Business Continuity Plans, KAU shall implement workable contingency plans for their systems that allow operational capabilities to be maintained or recovered in the event of sudden emergencies, including loss of staff, premises, equipment or key services. ➢ Contingency plans shall be developed to allow operational capabilities of their system to be recovered and in the event of interruption. ➢ KAU shall implement procedures to allow recovery and restoration of business operations and availability of information within the required time-scales. ➢ Business Continuity Department shall ensure the developed Business Continuity Management has identified sufficient financial, organizational, technical, and environmental resources to address the information security requirements. ➢ Business Continuity Department shall provide an overall approach to business continuity in line with the results of the business continuity analysis and risk assessment. ➢ Copies of Business Continuity Plans and their relevant materials shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster that might occur at the main site. KAU Management shall ensure that those copies are updated and protected with the same level of security as applied at the main site. ➢ Components which are critical to the continuity of service shall be identified, and business continuity plan shall include arrangements to enable services to be resumed promptly in the event of their failure. Some specific measures are listed below: • Provision of stand-by power supplies. • Duplication of processors and on-line storage. • Automatic re-routing of communications. • Fall-back to alternative internet carrier services. • Duplication of network operations centers. • Contract-based maintenance to ensure timely repair. ➢ Business Continuity Department shall annually review and update the Business Continuity Plans. ➢ Business Continuity Plans shall be developed to maintain or restore business operations in the required time scales following interruptions to, or failure of, critical business processes. The Business Continuity Planning process shall consider the following: • Identification and agreement of all responsibilities and emergency procedures. • Identification of the acceptable loss of information and services. • Implementation of emergency procedures to allow recovery and restoration in required time-scale. Particular attention needs to be given to external business dependencies and the contracts in place e.g. clinical systems suppliers, hardware maintenance contracts.

Policy Objective	Policy Statement
	• Clear and precise documentation of all agreed procedures and processes. • Appropriate training of staff in the agreed emergency procedures and processes, including crisis management. • Testing and updating plans. ➢ Business Continuity Plans shall address KAU vulnerabilities and therefore may contain sensitive information that needs to be appropriately protected. ➢ A single framework of business continuity plans shall be maintained by Business Continuity Department to ensure that all plans are consistent, to identify priorities for testing, maintenance and information security. ➢ KAU Business Continuity Planning framework shall cover the following: • The conditions for activating the plans (i.e., how to assess the situation, who is to be involved, etc.) before each plan is activated. • Emergency procedures, which describe the immediate action to be taken following an incident which jeopardizes business operations and/or human life. This shall include arrangements for media handling (to avoid/minimize the loss) and for effective liaison with appropriate public authorities (e.g. police, fire service and local government). • Fallback procedures to move essential business activities or support services to alternative temporary locations and to bring business processes back into operation in the required time-scales. • Procedures for the resumption of normal business operations. • Maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan. • Business Continuity training for the individuals is essential for effective resumption and recovery of operations. • The responsibilities of the individuals, describing who is responsible for executing each component of the plan. Alternates shall be nominated as required. As well as contact information such as telephone numbers and addresses for those individuals. • The critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures. ➢ Emergency procedures, manual fallback plans and resumption plans shall be the responsibility of the appropriate business owner. ➢ Business Continuity Plans shall be tested on a regular basis. The tests shall ensure that members of the recovery team and other relevant staff are aware of the plans. The test schedule for business continuity plans shall indicate how and when each element of the plan shall be tested. ➢ Business Continuity Plan shall use a variety of techniques in order to provide assurance that the plan (s) will operate in real life. These techniques shall cover the following: • Table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions). • Simulations (particularly for training people in their post-

Policy Objective	Policy Statement
	incident/crisis management roles). • Technical recovery testing (ensuring information systems can be restored effectively). • Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site). • Tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment). • Complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions). ➢ The results of Business Continuity Plan tests shall be recorded and actions taken to improve the plans, where necessary. ➢ Reporting Business Continuity Planning status and progress is a key element of creating an effective Business Continuity Plan program in the organization. The Information Security Department shall report the status and progress of the Business Continuity Planning program to the KAU management on a semi-annual basis or after every Business Continuity test.

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