Physical and Environmental Security Policy

King Abdulaziz University

Document Revision #: 1.0

Table of Contents

Policy Structure

1. Purpose

This policy establishes guidelines to prevent unauthorized access and interference to KAU premises and information assets. It also suggests guidelines to build security controls to prevent damage from physical security threats and environmental hazards.

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. Administration Department Role

- Establish and maintain physical access control systems.
- Perform physical security reviews.
- Design and supervise the installation, maintenance and operation of physical security systems.
- Design and supervise the installation and operation of environmental control systems.

- Assist or inform parties that are involved in case of changes of duties or employee termination.

- Participate in designing, Implementing and supervising of physical and environmental security controls.

3. 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.

- Access Control Policy.

- Asset Management Policy.

- Personnel Security Policy.

7. Owner

- Information Security Manager.

8. Policy Statement

Physical and Environmental Security protects information and information systems facilities from physical and environmental threats. KAU shall ensure that physical access to information processing areas and their supporting infrastructure (communications, power, and environmental) are controlled to prevent, detect, and minimize the effects of unintended access to these areas (e.g., unauthorized access, or disruption of processing itself).

This Policy addresses issues related to physical security perimeter, physical entry controls, working conditions, securing offices, data centers, equipment security and general controls.

1. Physical and Environmental Controls

Policy Objective	Policy Statement
Prevent unauthorized physical access, damage and interference to the organization's premises and information [A.9.1]	➢ The physical layout of KAU's information processing facilities shall be segregated into perimeter zones. Each zone shall have a higher level of access restrictions and access authorization requirements. ➢ Secure zones shall have strict physical security to provide additional protection to those assets. Physical access controls shall be in place using walls, access doors with secure locks or a security desk. Based on the criticality of the protected assets the choice of the physical access controls can be made. ➢ The security perimeter shall be clearly defined and implemented. ➢ A manned reception area or other means to control physical access to the site or building shall be in place. Access to the sites and buildings shall be restricted to authorized personnel only. ➢ Physical barriers shall, if necessary, be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding. ➢ All fire doors on a security perimeter shall be alarmed; and shall slam shut. ➢ The perimeter of a building or site containing information processing facilities shall be physically sound. ➢ Access to high security areas such as data centers shall be restricted to those individuals with direct responsibility for the operation and maintenance of that data center. ➢ All personnel shall be required to wear some form of visible identification. ➢ All KAU employees shall not be sharing their security access

Policy Objective	Policy Statement
	cards to KAU premises. ➢ Access rights to secure areas shall be regularly reviewed and updated. ➢ Access to sensitive information and information processing facilities shall be controlled and restricted to authorized persons only. An audit trail of all access shall be securely maintained. ➢ All visitors to KAU's information processing facilities shall sign-in with the security guard in a "Visitor Log" that is retained and reviewed; and KAU shall implement visitor control procedures. ➢ Information processing facilities managed by the KAU shall be physically separated from those managed by third parties. ➢ Surveillance monitoring shall be installed in information processing facility and monitored. ➢ Suitable intruder detection systems shall be installed and regularly tested to cover all external doors and accessible windows. ➢ Support functions and equipment (e.g. photocopiers and fax machines) shall be sited appropriately within the secure area to avoid demands for access, which could compromise information. ➢ Hazardous or combustible materials shall be stored securely at a safe distance from a secure area. ➢ Fallback equipment and backup media shall be sited at a safe distance to avoid damage from a disaster at the main site. ➢ Environmental controls shall be designed and applied to minimize the damage resulting from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or human-caused disasters. ➢ KAU shall provide the level of physical and environmental protection of its technical infrastructure to minimize the risk of environmental hazards. ➢ The design of environmental controls shall take into account relevant health and safety regulations and standards, and shall consider security threats presented by neighbouring premises. ➢ The KAU shall ensure that: • The information processing facilities are not located in an environmentally unstable area. • The information processing facilities are not located near any dangerous neighbouring facilities (e.g.

Policy Objective	Policy Statement
	chemical laboratories, etc.) • The installed fire detection and fighting equipment meet the requirements defined by the manufacturers. ➢ KAU shall observe personnel safety as a high priority and take the necessary steps to ensure a safe workplace. KAU shall develop, in collaboration with other responsible division/offices, appropriate emergency procedures for handling a variety of threats. Emergency procedures shall be documented, maintained and tested periodically at each facility for each significant threat. ➢ KAU facilities shall contain emergency equipment (e.g., emergency lighting, fire extinguishers) to establish an adequate level of safety for those working within a facility. This equipment shall be inspected annually to ensure its operational capabilities. ➢ Controls and guidelines shall be made available to enhance the security of a secure area. This shall apply to employees as well as contractors and third parties working in the secure area. ➢ Work in secure area done by third party and vendors shall be monitored and supervised. ➢ Monitoring at KAU site shall be performed to ensure workforce safety and prevent property loss. ➢ Third party support services personnel shall not be granted access to secure areas unless it is required, authorized, and supervised.

2. Asset Security

Policy Objective	Policy Statement
Prevent loss, damage, theft or compromise of assets and interruption to the organization's activities [A.9.2]	➢ The Information processing facilities of KAU which are processing sensitive data shall be isolated to apply further controls. ➢ All the environmental conditions that affect the operation of KAU sensitive information processing facilities shall be monitored (e.g. heat and humidity). ➢ The telecommunications lines and equipment of KAU shall be adequately protected to ensure both availability and the confidentiality of this resource. ➢ Any movement of information, software media, hardware or

Policy Objective	Policy Statement
	other physical assets shall be strictly controlled. Only authorized personnel shall be permitted to take KAU property off the premises and they shall be responsible for protecting the property and controlling its use. KAU shall develop and maintain appropriate procedures for its property control. ➢ KAU shall provide power protection to support both personnel safety and ensure the availability of its information systems. All critical applications shall be configured to switchover to an alternate power source immediately upon loss of power. ➢ Power cables shall be segregated from communications cables to prevent interference. ➢ Network cabling shall be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas. ➢ Any preventive and corrective maintenance conducted by the supplier's personnel to KAU shall be supervised and formal approval shall be obtained. ➢ KAU shall properly maintain equipment to ensure its continued availability and integrity. ➢ Information Security Department shall ensure that proper procedures for off-site placement are carried according to safety requirements specific to that information asset. ➢ The off-site storage facilities for KAU shall be afforded the same level of protection as the main processing site. Adequate physical security and environmental controls shall be implemented to protect the data. ➢ Equipment and media taken off the premises shall not be left unattended in public places. ➢ Security for the equipment used off of KAU premises shall be the same as the security used for on-site equipment, taking into account the risks of working outside the organization's premises. ➢ Storage devices containing sensitive information shall be physically destroyed or securely overwritten rather than using the standard delete function. ➢ KAU sensitive documents, media and equipment shall be disposed of in an approved manner that protects the confidentiality of the information printed or stored. ➢ Damaged storage devices containing sensitive data may require a risk assessment to determine if the items shall be destroyed,

Policy Objective	Policy Statement
	repaired or discarded. ➢ Written authorization shall be obtained for equipment, information or software taken off- KAU premises. ➢ KAU shall maintain an accurate and updated records of all equipment moved off-premises.

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