INSPIRING BUSINESS INNOVATION

جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

Physical and Environmental Security Policy

Version: 2.0

Policy Code: DICT-QAP017

October 2020

All rights reserved for Deanship of ICT ©

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Table of Contents

Property Information 3
Document Control 4
Information 4
Revision History 4
Distribution List 4
Approval 4
Policy Overview 5
Purpose 5
Scope 5
Terms and Definitions 5
Change, Review and Update 8
Enforcement / Compliance 8
Waiver 8
Roles and Responsibilities (RACI Matrix) 9
Relevant Documents 10
Ownership 10
Policy Statements 11
Confidentiality of Information 11
Physical Security Parameter 12
Physical Entry Controls 14
Securing Offices, Rooms and Facilities 15
Protecting against External and Environmental Threats 15
Working in Secure Areas 16
Delivery and Loading Areas 17
Equipment Siting and Protection 17
Supporting Utilities 19
Cabling Security 19
Equipment Maintenance 20
Removal of Assets 21
Security of Equipment and Assets Off-Premises 21
Secure Disposal or Re-use of Equipment 22
Unattended User Equipment 23
Clear Desk and Clear Screen Policy 23

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Property Information

This document is the property information of Imam Abdulrahman bin Faisal University - ICT Deanship. The content of this document is intended only for the valid recipients. This document is not to be distributed, disclosed, published or copied without ICT Deanship written permission.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Document Control

Information

Title	Classification	Version	Status
PHYSICAL AND ENVIRONMENTAL SECURITY POLICY	Public	2.0	validated

Revision History

Version	Author(s)	Issue Date	Changes
0.1	Alaa Alaiwah – Devoteam	November 17, 2014	Creation
0.2	Nabeel Albahbooh – Devoteam	December 1, 2014	Update
0.3	Osama Al Omari – Devoteam	December 23, 2014	QA
1.0	Nabeel Albahbooh – Devoteam	December 31, 2014	Update
1.1	Muneeb Ahmad – ICT, IAU	09 May 2017	Update
1.2	Lamia Abdullah Aljafari	6 June 2020	Update
2.0	Dr. Samer Bani Awwad	13 September 2020	Update

Distribution List

#	Recipients
1	Legal Affairs
2	Website
3	Quality Assurance Department - DICT
4	Department of Administrative and Finance Affairs - DICT

Approval

Name	Title	Date	Signature
Dr. Khalid Adnan Alissa	Dean of DICT	8th October 2020	

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Policy Overview

This section describes and details the purpose, scope, terms and definitions, change, review and update, enforcement / compliance, wavier, roles and responsibilities, relevant documents and ownership.

Purpose

The main purpose of **Physical and Environmental Security Policy** is to:

Prevent unauthorized physical access, damage and interference to IAU's information and information processing facilities, and to prevent loss, damage, theft or compromise of assets and interruption to IAU's operations.

Scope

The policy statements written in this document are applicable to all IAU's resources at all levels of sensitivity; including:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of IAU.
- Students studying at IAU.
- Contractors and consultants working for or on behalf of IAU.
- All other individuals and groups who have been granted access to IAU's ICT systems and information.

This policy covers all information assets defined in the *Risk Assessment Scope Document* and will be used as a foundation for information security management.

Terms and Definitions

Term	Definition
Accountability	A security principle indicating that individuals shall be able to be identified and to be held responsible for their actions.
Asset	Information that has value to the organization such as forms, media, networks, hardware, software and information system.
Availability	The state of an asset or a service of being accessible and usable upon demand by an authorized entity.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Confidentiality	An asset or a service is not made available or disclosed to unauthorized individuals, entities or processes.
Control	A means of managing risk, including policies, procedures, and guidelines which can be of administrative, technical, management or legal nature.
Guideline	A description that clarifies what shall be done and how, to achieve the objectives set out in policies.
Need to Know	A user is only granted access to the information he needs to perform his tasks (different tasks/roles mean different need-to-know and hence different access profiles).
Need to Use	A user is only granted access to IT facilities (e.g., equipment, applications, procedures and rooms) he needs to perform his task/job/role.
Information Security	The preservation of confidentiality, integrity, and availability of information. Additionally, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
Integrity	Maintaining and assuring the accuracy and consistency of asset over its entire life-cycle.
Owner	A person or group of people who have been identified by Management as having responsibility for the maintenance of the confidentiality, availability and integrity of an asset. The Owner may change during the lifecycle of the asset.
Policy	A plan of action to guide decisions and actions. The policy process includes the identification of different alternatives such as programs or spending priorities, and choosing among them on the basis of the impact they will have.
Provisioning	A process of assigning or revoking access rights for users to information, systems and services.
Risk	A combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
System	An equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, control, display, switching, interchange, transmission or reception of data and that includes computer software, firmware and hardware.

Table 1 provides definitions of the common terms used in this document.

Term	Definition
Accountability	A security principle indicating that individuals shall be able to be identified and to be held responsible for their actions.
Asset	Information that has value to the organization such as forms, media, networks, hardware, software and information system.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Availability	The state of an asset or a service of being accessible and usable upon demand by an authorized entity.
Confidentiality	An asset or a service is not made available or disclosed to unauthorized individuals, entities or processes.
Control	A means of managing risk, including policies, procedures, and guidelines which can be of administrative, technical, management or legal nature.
Guideline	A description that clarifies what shall be done and how, to achieve the objectives set out in policies.
Need to Know	A user is only granted access to the information he needs to perform his tasks (different tasks/roles mean different need-to-know and hence different access profiles).
Need to Use	A user is only granted access to IT facilities (e.g., equipment, applications, procedures and rooms) he needs to perform his task/job/role.
Information Security	The preservation of confidentiality, integrity, and availability of information. Additionally, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
Integrity	Maintaining and assuring the accuracy and consistency of asset over its entire life-cycle.
Owner	A person or group of people who have been identified by Management as having responsibility for the maintenance of the confidentiality, availability and integrity of an asset. The Owner may change during the lifecycle of the asset.
Policy	A plan of action to guide decisions and actions. The policy process includes the identification of different alternatives such as programs or spending priorities, and choosing among them on the basis of the impact they will have.
Provisioning	A process of assigning or revoking access rights for users to information, systems and services.
Risk	A combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
System	An equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, control, display, switching, interchange, transmission or reception of data and that includes computer software, firmware and hardware.

Table 1: Terms and Definitions

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Change, Review and Update

This policy shall be reviewed **once every year** unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes of this policy shall be exclusively performed by the Information Security Officer and approved by management. A change log shall be kept current and be updated as soon as any change has been made.

Enforcement / Compliance

Compliance with this policy is **mandatory** and it is to be reviewed periodically by the Information Security Officer. All IAU units (Deanship, Department, College, Section and Center) shall ensure continuous compliance monitoring within their area.

In case of ignoring or infringing the information security directives, IAU's environment could be harmed (e.g., loss of trust and reputation, operational disruptions or legal violations), and the fallible persons will be made responsible resulting in disciplinary or corrective actions (e.g., dismissal) and could face legal investigations.

A correct and fair treatment of employees who are under suspicion of violating security directives (e.g., disciplinary action) has to be ensured. For the treatment of policy violations, Management and Human Resources Department have to be informed and deal with the handling of policy violations.

Waiver

Information security shall consider exceptions on an individual basis. For an exception to be approved, a business case outlining the logic behind the request shall accompany the request. Exceptions to the policy compliance requirement shall be authorized by the Information Security Officer and approved by the ICT Deanship. Each waiver request shall include justification and benefits attributed to the waiver.

The policy waiver period has maximum period of 4 months, and shall be reassessed and re-approved, if necessary for maximum three consecutive terms. No policy shall be provided waiver for more than three consecutive terms.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Roles and Responsibilities (RACI Matrix)

Table ***2*** shows the RACI matrix[1] that identifies who is responsible, accountable, consulted or informed for every task that needs to be performed.

There are a few roles involved in this policy respectively: ICT Deanship, Information Security Officer (ISO), Human Resources Department / Administrative Unit (HR/A), Operations and Maintenance Department (O&M), Security and Safety Department (S&S), Owner and User (Employees, Faculty Members, Students, Contractors, Consultants and Third Parties).

Roles / Responsibilities	ICT	ISO	HR/A	O&M	S&S	Owner	User
Defining the necessary policies and procedures regarding physical access to IAU's sensitive information.	C	R,A				C	
Providing electrical supply and power protection to IAU's ICT facilities.	C,I	C		R,A			
Maintaining hardware equipment in accordance with the manufacture's guidelines.	C,I	C		R,A			
Determining the required access rights of users to assets.	R,C	C		C		R,A	I
Defining and implementing the appropriate controls for physical access protection.	R,A	C,I			R,A		
Ensuring personnel safety and a safe workplace within IAU's environment.	R,A	C	R,C,I		R,A		
Implementing appropriate controls to protect the confidentiality, integrity and authenticity of sensitive information.	R,A				R,A		
Establishing and maintaining physical access control systems.							
Designing and supervising the installation, maintenance and operation of physical security systems and environmental control systems.							
Performing physical security reviews.	R,A	C,I			R,A		
Implementing proper controls to protect assets.	R,A	C,I			R,A		

Table 2: Assigned Roles and Responsibilities based on RACI Matrix

[1] The responsibility assignment RACI matrix describes the participation by various roles in completing tasks for a business process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental processes. R stands for Responsible who performs a task, A stands for Accountable (or Approver) who sings off (approves) on a task that a responsible performs, C stands for Consulted (or Consul) who provide opinions, and I stands for Informed who is kept up-to-date on task progress.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Relevant Documents

The following are all relevant policies and procedures to this policy:

- Information Security Policy
- Human Resource Security Policy
- Asset Management Policy
- Access Control Policy
- Compliance Policy
- Asset Management Procedure
- Human Resource Security Procedure
- Physical and Logical Access Control Procedure

Ownership

This document is owned and maintained by the ICT Deanship of University of Imam Abdulrahman bin Faisal.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Policy Statements

The following subsections present the policy statements in 15 main aspects:

Physical Security Parameter

Physical Entry Controls

Securing Offices, Rooms and Facilities

Protecting against External and Environmental Threats

Working in Secure Areas

Delivery and Loading Areas

Equipment Siting and Protection

Supporting Utilities

Cabling Security

Equipment Maintenance

Removal of Assets

Security of Equipment and Assets Off-Premises

Secure Disposal or Re-use of Equipment

Unattended User Equipment

Clear Desk and Clear Screen Policy

Confidentiality of Information

1. Users shall exercise all necessary due care in protecting IAU's assets. Each user shall have the responsibility to:
    a. Prevent unauthorized access, including viewing of information resources under his responsibility or control (such as information available on laptops, desktop computers, access terminals, printouts or tape media etc.).
2. Users shall display their identification badges (ID cards) at all the times on IAU's premises.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Physical Security Parameter

1. The choice and application of physical access controls shall be made according to the classification of the protected system such as:
    a. Perimeter fences or walls, bounds and checkpoints.
    b. Key locks to be opened with ordinary keys (i.e., non-electronic).
    c. Electronic access control systems:
        - Option 1 – Cipher lock (also known as programmable lock use keypads to control access).
        - Option 2 – Card based access control:
            - Memory card (e.g., magnetic card).
            - Smart card (includes microchip).
        - Option 3 – Biometric systems (e.g., fingerprint, hand geometry and face recognition).
        - Any combination of option 1, 2 or 3 (i.e., a multi-factor authentication method).
2. The physical layout of ICT Deanship shall be segregated into perimeter zones. Each zone shall have its own defined level of access restrictions and access authorization requirements. The perimeter zones may include, but not be limited to:

Zone	Description	Access Control Measures
Public Zone and/or Reception Zone	Limited restrictions – area under overall surveillance	• Perimeter fences or walls, bounds and 24 x 7 perimeter checkpoint. • Randomized identity checks on physical perimeter.
Office Zone	Limited access – registration with reception required	• A single factor (electronic) access control system (e.g., memory card and physical key). • Employee shall be personally identifiable in case of electronic access control.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Zone	Description	Access Control Measures
ICT Admins Secure Access Zone	Limited access – registration with reception required and area under overall surveillance	• Where possible, a multi-factor electronic access control device (e.g., fingerprints and passes code, smart card and pass code).
Main Datacenter Restricted Access Zone	Specifically, authorized personnel only – highly restricted access, logged access, specific authorization required for engineers, technicians and visitor access and area under surveillance	• Installing walls, access doors with secure locks or a security desk. • Where possible, multi-factor electronic access control device (e.g., fingerprint and pass code, smart card and pass code).

3. Sites that host sensitive information and critical systems shall have additional physical security zones to provide additional protection to those assets.
4. Access rights to secure areas shall be regularly reviewed and updated.
5. Main Datacentre area within IAU's environment:
    a. Shall require a much greater level of control than other restricted IAU's spaces.
    b. Individuals who are granted authorization from ICT Deanship may enter this area.
    c. Access privileges shall only be granted to individuals who have legitimate business needs.
    d. Shall be entered only to conduct authorized business works.
    e. Employees having access shall familiarize themselves thoroughly with this policy.
6. All doors to Datacentre shall remain locked at all times; and may only be temporarily opened for periods not to exceed that is minimally necessary in order to:
    a. Allow officially approved and logged entrance and exit of authorized individuals.
    b. Permit the transfer of supplies / equipment as directly supervised by a person with controlling access to the area.
    c. Prop open a door to Datacentre only if it is necessary to increase airflow into it if an air conditioning fails.

[ISO/IEC 27001: A.11.1.1]

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Physical Entry Controls

1. Security and Safety Department in cooperation with ICT Deanship and Information Security Officer shall be responsible for defining the necessary policies and procedures regarding physical access to buildings and areas where IAU's systems are sited (e.g., Datacentre), according to the classification of the protected systems.
2. The entry and exit of visitors shall be controlled. Before a visitor enters a building, the security guards at the reception desk or gate shall verify the visitor identity using generally accepted credential (e.g., an Identity Card or Passport). Entry shall be allowed only after notifying the employee to whom the visitor is visiting and verifying the purpose of the visit.
3. Supporting services contractors' personnel shall be granted a restricted access to secure areas or Datacentre's facilities only when required; and it shall be monitored.
4. For employee's identification, the followings shall be considered:
    a. All IAU's employees shall wear visible identification (e.g., ID badge).
    b. Persons who are not IAU's employees shall wear a "Visitor" badge.
    c. ID badges shall only contain names, photographs and badge numbers.
    d. Access cards shall not contain any description of access privilege levels granted to that card.
5. ICT Deanship in cooperation with Security and Safety Department shall be responsible for managing and monitoring CCTV cameras and access doors systems within Datacenter.
6. All entries to Datacenter shall be recorded and maintained for at least 6 months. All access logs shall record the following details:
    a. The date and time of the access attempt.
    b. Whether the attempt was successful or not.
    c. Where access was granted (which door for example).
    d. Who attempted the access.
    e. Who modified the access privileges at the supervisor level.
7. Personnel who do not require continuing access to Datacenter shall be escorted by an authorized employee at all times and shall be required to sign a visitor control log.
8. A facility-wide access card control system shall be deployed with the following features:

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

a. Employee identification and/or access card with picture.

b. Logging activity associated with each computerized card.

c. Assign access rights based upon job requirements.

d. Ability to disable lost or stolen cards.

[ISO/IEC 27001: A.11.1.2]

Securing Offices, Rooms and Facilities

1. Facilities security shall be provided at all IAU's departments, units and offices. This shall include, but not be limited to:
    a. Site perimeter protection (e.g., smart cards).
    b. Facility management.
    c. Parking lot security.
2. The facilities where sensitive information and critical systems are stored or processed shall be constructed and arranged in a way that they are adequately protected from physical and environmental threats.
3. Intrusion detection alarms shall be in place to cover external doors and accessible windows and other access points to IAU's buildings.
4. Hazardous or combustible materials shall be stored securely at a safe distance from a secure area.

[ISO/IEC 27001: A.11.1.3]

Protecting against External and Environmental Threats

1. Security and Safety Department shall observe personnel safety as a high priority and take the necessary steps to ensure a safe workplace.
2. Proper procedures regarding the safe evacuation of areas or building in case of fire, flood, earthquake or other disasters shall be developed and documented in order to protect IAU's employees and systems.
3. 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.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

4. IAU's facilities shall contain emergency equipment (e.g., emergency lighting, and fire extinguishers) to establish an adequate level of safety for those working within a facility. This equipment shall be inspected in annual basis in order to ensure their operational capabilities.
5. Areas where Datacenter is located shall have appropriate external and environmental controls in place (e.g., temperature, humidity, dust particle content, atmospheric pressure, electromagnetic radiation, or static electricity) according to the manufacturer's recommendations.
6. ICT Deanship shall be responsible for the physical monitoring of Datacenter. In particular, the following assets shall be centrally monitored:
    a. Physical access control.
    b. Ventilation and Air-Conditioning.
    c. Emergency power supply (i.e. power generator) and UPS.
    d. Fire detection and suppression systems.
    e. Water detection system.
    f. CCTV.
    g. Racks.

[ISO/IEC 27001: A.11.1.4]

Working in Secure Areas

1. Security and Safety Department in cooperation with ICT Deanship and Information Security Officer shall define what areas are (e.g., Datacenter) to be treated as secure areas in order to minimize unauthorized access, damage and interference to assets.
2. Areas that host sensitive information, critical information systems and infrastructure shall be continuously monitored via security guards, Closed Circuit TV (CCTV), intrusion detection systems or a combination of them.
3. All storage media (e.g., hard disk drives, CD-ROMs or DVDs), printouts, manuals and generally information in printed form containing sensitive information shall be physically secured in locked drawers and cabinets when not in use.
4. Controls for individuals working in secure areas shall include, but not be limited to:

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

a. Un-staffed secure areas are physically locked and periodically monitored.

b. No photographic, video, audio, smart phones or other recording equipment is allowed unless specifically authorized.

c. Third party support services personnel are granted access to secure areas only when required, authorized and supervised.

[ISO/IEC 27001: A.11.1.5]

Delivery and Loading Areas

1. Delivery and loading areas shall be controlled and, if possible, isolated from ICT facilities to avoid unauthorized access or causing destruction to sensitive areas. Security requirements that control delivery and loading area shall include, but not be limited to:

    a. Access to a loading area from outside of IAU's premises shall be restricted to identified and authorized personnel.

    b. The loading area shall be designed in which supplies can be unloaded without delivery staff gaining access to other areas of IAU's premises.

2. All incoming packages to IAU's premises shall be received by reception staff to be inspected. Also, they shall be recorded in a register.

[ISO/IEC 27001: A.11.1.6]

Equipment Siting and Protection

1. Based on information and/or systems classification, equipment shall be protected to reduce risks from environmental threats and hazards; and to reduce the risk of unauthorized access to information.

2. The followings controls shall be considered to secure all critical systems:

    a. Equipment is located in a physically secure location to minimize unauthorized access.

    b. Environmental conditions are monitored for conditions that could adversely affect the operation of computer systems.

    c. System owners need to consider potential impact of a disaster happening in nearby premises (e.g., a fire in a neighbouring building or water leaking from the roof or in floors below ground level or an explosion in the street).

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

3. ICT facilities shall be located based on the following, but not be limited to:
    a. Not at locations accessible by public.
    b. Not at locations prone to natural disasters or damage caused by individuals such as vandalism, fires and accidents (e.g., from water supply system failures or water entering from external windows).
4. All ICT equipment (e.g., servers and network devices) shall be physically located within the protected confines of Datacentre.
5. Unauthorized system access via bypass booting of the device (to defeat password authentication) shall be prevented.
6. Security measures shall be implemented to minimize the risk of information leakage from equipment processing sensitive information.

[ISO/IEC 27001: A.11.2.1]

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Supporting Utilities

1. ICT Deanship in cooperation with Operation and Maintenance Department shall provide power protection to ensure the availability of IAU's systems.
2. To achieve continuity of power supplies, the followings shall be considered, but not be limited to:
    a. Multiple feeds to avoid a single point of failure in the power supply.
    b. Uninterruptable Power Supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical systems and business operations. UPS shall be regularly tested, as per vendor's instructions, to ensure reliable functionality.
    c. A backup generator is considered when processing and business continuity is required.
3. All critical systems shall be configured to switchover to an alternate power source immediately upon loss of power.
4. Equipment shall be protected from power failures and other electrical anomalies. A suitable electrical supply shall be provided in accordance with equipment manufacturer's specifications.
5. Supporting infrastructure (e.g., air conditioning systems and security alarm systems), where applicable, shall have a dependable and consistent electrical power supply that is free from surges and interference that shall affect operation of the equipment (e.g., power-conditioning strips could reduce the threat of power surges).
6. UPS shall be regularly tested, as per vendor's instructions, to ensure reliable functionality.

[ISO/IEC 27001: A.11.2.2]

Cabling Security

1. Power, voice and telecommunication cables shall be protected against physical damage and destruction.
2. Cabling protection shall include, but not be limited to:
    a. Telecommunication cabling is protected against wiretapping.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

b. Telecommunication cabling is not passed through areas where third parties have access.

c. Data network cabling is adequately isolated and protected from unauthorized interception or damage via routing them through protected areas.

d. Power supply cabling is adequately isolated.

e. Installation of armoured conduit and locked rooms or boxes at inspection and termination points.

f. Use of alternative routings or transmission media.

g. Use of fiber optic cabling.

h. Initiation of sweeps for unauthorized devices being attached to the cables.

3. Where possible, cabling shall be run underground, avoid public areas, and use conduit protective shielding.

[ISO/IEC 27001: A.11.2.3]

Equipment Maintenance

1. ICT Deanship in cooperation with Operations and Maintenance Department shall properly maintain technical equipment (e.g., hardware servers, network devices, racks, patch panels, communication devices, cables, etc.) to ensure their continued availability and integrity. Equipment maintenance controls shall include, but not be limited to:

    a. Maintaining equipment in accordance with the manufacture's recommended service intervals and specifications.

    b. Permitting only authorized maintenance personnel to carry out repairs and service.

    c. Recording and updating all suspected or actual equipment faults and all preventive and corrective maintenance.

2. Any preventive and corrective maintenance conducted by the manufacture's personnel to ICT equipment shall be supervised and a formal approval shall be obtained.

3. The followings shall be considered for ICT equipment:

    a. All ICT equipment, if possible, shall have a mandatory maintenance contracts to ensure availability and continuity of business.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

b. Maintenance contracts shall cover regular and emergency checks.

c. ICT equipment shall have a valid maintenance contracts which covers regular checks, support and spare parts.

d. Maintenance activities shall be supervised by respective personnel.

e. Vendors shall provide IAU with maintenance reports on monthly basis to ensure proper health status of the equipment.

f. Datacentre maintenance schedule and a log shall be maintained by ICT Deanship to ensure on time maintenance and tracking of any related issues.

[ISO/IEC 27001: A.11.2.4]

Removal of Assets

1. ICT equipment, assets or software shall not to be taken off-site IAU without a proper authorization. Where necessary and appropriate, the followings shall be considered:

    a. Personal shall obtain a proper authorization to take equipment off-site IAU.

    b. Equipment is logged out.

    c. Time limits are set.

    d. When returned, equipment is logged back in.

[ISO/IEC 27001: A.11.2.5]

Security of Equipment and Assets Off-Premises

1. ICT Deanship shall implement appropriate controls when sending ICT equipment off IAU's premises for maintenance. Appropriate controls shall include, but not be limited to:

    a. Proper packaging and sealing of containers.

    b. Storage in safe and secure places.

    c. Clear and complete shipping and tracking instructions.

2. Assets shall not be moved off IAU's premises for use maintenance or repair purpose unless authorization has been obtained from the relevant owner of the information asset. All movement of such asset shall be recorded.

3. All portable ICT equipment (e.g., laptops and mobile phones):

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

a. Shall be secured by means of a locked cabinet, credenza, vinyl-covered steel cable or office.

b. Shall be physically secured via an appropriate security device during any period that the unit is left unattended in IAU's offices.

4. Portable ICT equipment connected to the network shall store sensitive information on file server drives as much as possible. Information stored on floppy disks, CD-Rooms, external drives or tapes shall be physically secured in a manner appropriate to its sensitivity level.

[ISO/IEC 27001: A.11.2.6]

Secure Disposal or Re-use of Equipment

1. ICT Deanship shall develop appropriate procedures for the followings:

   a. Disposal of confidential documents.

   b. Destruction of computer equipment that may contain sensitive information.

   c. Sanitization (i.e., object reuse) of equipment that might be sold or transferred to other organization.

   d. Destruction of various types of media.

2. Storage media (e.g., CD-ROMs, tapes and flash memories) that contains sensitive information that no longer needs to be kept shall be physically destroyed as follows:

   a. Rewriteable media is erased using a secure procedure (e.g., through multiple overwrites, may be three or more times) to prevents the data from later being scavenged.

   b. Paper document is destroyed using paper shredders.

3. ICT Deanship shall maintain disposal records which include the information owner's disposal request and the corresponding department director's approval.

4. ICT equipment and storage media shall be checked prior to disposal or re-use to ensure that sensitive information and licensed software has been removed or securely overwritten.

5. Destruction of sensitive information captured on storage media shall only be performed after approval has been obtained for the method of destruction.

[ISO/IEC 27001: A.11.2.7]

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

Unattended User Equipment

1. ICT Deanship shall enable screen saver password on all servers and workstations to prevent unauthorized access. The screen saver timer shall be set to 10 minutes of inactivity or less.
2. Each user shall terminate active sessions when activities are finished.
3. Each user shall lock his equipment before leaving his desk.

[ISO/IEC 27001: A.11.2.8]

Clear Desk and Clear Screen Policy

1. At a minimum, the following guidelines shall be followed and implemented by all users to promote clear desk and clear screen policy:
    a. Paper and information media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside normal working hours.
    b. Sensitive or critical business documentations shall be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.
    c. Workstations and printers shall not be left logged on when unattended; and shall be protected by password protected screen savers.
    d. Photocopiers and faxes shall be locked (e.g., protected from unauthorized use through PIN code function) outside normal working hours.
    e. Confidential information, when printed, shall be immediately cleared from printers.
2. Department Managers shall communicate the clear desk and clear screen policy to the employees in their own areas; and shall periodically monitor their activities to ensure users compliance.
3. Information Security Officer in cooperation with Personnel Affairs Department shall ensure that proper awareness training addresses clear desk and clear screen policy is delivered to all IAU's employees.

[ISO/IEC 27001: A.11.2.9]

---------- End of Document ----------

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©