جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

Physical and Environmental Policy

Version: 2.0

CODE: DICT.I.06-32.CS.E.V2.0

1 Table of Cont.

1 Table of Cont. 2
2 Intellectual Property Information 4
3 Document Control 5
3.1 Information....5
3.2 Revision History 5
3.3 Document Review 5
3.4 Distribution List....5
3.5 Approval 5
4 Introduction:....6
5 Scope: 6
6 Policy Objectives: 6
7 Applicability and Scope:....6
8 Policy: 6
8.1 Physical Security Scope:....6
8.2 Physical Access Controls:....7
8.3 Visitor Access Controls: 8
8.4 Securing Workspaces:....9
8.5 Protection from Environmental and External Threats:.... 10
8.6 Equipment Security: 11
8.7 Supporting Facilities:.... 12
8.8 Cable Security: 13
8.9 Equipment Maintenance: 13
8.10Security of Device Usage Outside the IAU: 15
8.11Managing Removable Media and Handling:.... 15
8.12Secure Device Disposal and Reuse:.... 16
8.13Asset Removal and Physical Media Transfer Controls:.... 16
8.14Dealing with Transactions Outside of Official Working Hours:.... 17
9 Roles and Responsibilities: 17
10 Ownership of the Policy: 19
11 Changes to the Policy: 19

12 Compliance: 19
13 Related Policies, standards and Procedures 20
14 References.. 21

2 Intellectual Property Information

This document is the intellectual property of the Deanship of Information and Communication Technology (DICT) at Imam Abdulrahman bin Faisal University (IAU). The content of this document is intended solely for authorized recipients. Any distribution, disclosure, publication, or copying of this document without written permission from DICT is strictly prohibited.

3 Document Control

3.1 Information

Title	Classification	Version	Status
PHYSICAL AND ENVIRONMENTAL POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	17/02/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	19/05/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	21/12/2023	REVIEW AND UPDATE

3.3 Document Review

Date of Next Scheduled Review
01/01/2025

3.4 Distribution List

#	Recipients
1	ALL DICT DEPARTMENTS
2	LEGAL AFFAIRS
3	IAU WEBSITE
4	

3.5 Approval

Name	Position Title	Decision Number	Date
DR. NIHAD AL-OMAIR	VICE PRESIDENT OF DEVELOPMENT AND COMMUNITY PARTNERSHIP	61945	06/03/2024

4 Introduction:

Protecting information and its assets is a fundamental element for the success of the IAU. To achieve this goal, the Cybersecurity Management oversees the necessary security operations to safeguard the information and technological assets of the IAU. This document establishes the Physical Access Policy within the IAU, as well as defining physical and environmental security based on best practices and relevant legislative requirements.

5 Scope:

This policy is included within the framework of the IAU's policies and under the authority granted by the authorized entity, effective from the date of its adoption.

6 Policy Objectives:

The Physical and Environmental Cybersecurity Policy aims to enhance protective measures for the facility and its information and technological assets against potential threats or risks. It also establishes requirements for physical access, control, and monitoring.

7 Applicability and Scope:

The provisions of this policy apply to all affiliates or individuals working within the IAU, whether under permanent or temporary contracts, and whether directly or indirectly. This includes suppliers, external contractors, and any person with permanent or temporary access rights to the IAU's data, regardless of its source, format, or nature, as well as to the IAU's systems, devices, and databases.

8 Policy:

8.1 Physical Security Scope:

8.1.1 Necessary security requirements must be implemented for accessing sensitive facilities within the IAU, including personnel identification and verification of required access permits.

8.1.2 Physical measures should be provided to secure the IAU, such as fences, gates, and security barriers, to ensure the safety of information, data, and personnel.

8.1.3 The physical security scope must encompass the entire IAU, including entry points to buildings equipped with Closed-Circuit Television (CCTV) cameras, whenever possible, to monitor any suspicious activities or external threats.

8.1.4 All main entry/exit gates must be safeguarded against unauthorized access using control mechanisms such as barriers, alarm devices, appropriate locks, and others. Additionally, windows and doors in unoccupied work areas should be locked.

8.1.5 Explosive and metal detection screening devices should be provided at entry points, and specific instructions for inspecting bags must be enforced.

8.2 Physical Access Controls:

8.2.1 All main entry and exit gates of sensitive buildings within the university must be staffed with security personnel around the clock. The Security and Safety department should be responsible for appropriate tasks and informed accordingly. Reception or relevant personnel must be promptly notified of any suspicious activities or unauthorized external access.

8.2.2 All external doors and fences should be equipped with suitable devices (such as surveillance cameras, smart locks, etc.) to secure and regularly monitor the internal security scope.

8.2.3 All personnel within the university must wear identification cards (access permits) at all times, ensuring visibility.

8.2.4 The Security and Safety department must document all activities related to the creation and disposal of identification cards (access permits) in a dedicated Log Sheet.

8.2.5 Individuals without proper identification cards (access permits) are prohibited from accessing any sensitive facilities unless approval is granted by relevant departments.

8.2.6 The Cybersecurity and responsible personnel should periodically review the current list of affiliates holding access permits for sensitive facilities.

8.2.7 Access to important and sensitive areas (such as communication rooms and data processing areas) should be restricted to authorized personnel only.

8.2.8 Categorization of university facilities should be based on the classification of the handled and processed information.

8.2.9 External parties must not be granted access to important and sensitive areas unless necessary. Security access licenses should be issued in coordination with relevant departments. External parties should be accompanied by the benefiting department and continuously monitored during their presence in important and sensitive locations.

8.2.10 Records of entry to sensitive areas must be maintained and periodically reviewed according to the Asset Management policy, immediately notifying the Cybersecurity and Security & Safety departments and facilities of any suspicious activities or clear security violations.

8.2.11 Access to loading and unloading areas at IAU sites should be restricted to authorized personnel only.

8.2.12 All incoming materials should be inspected for hazardous substances or potential threats before being transported from the loading and unloading areas to their intended destinations.

8.2.13 All outgoing and incoming materials must be logged according to the Asset Management policy upon their arrival at the site.

8.2.14 Sensitive areas such as data centres, generator rooms, backup power sources (UPS), air handling units, and locations where important and sensitive information is processed should be equipped with multi-factor authentication systems, such as access control cards and biometric traits like fingerprint recognition.

8.2.15 Access cards must be deactivated upon an affiliate's resignation, contract termination, or transfer to another entity.

8.2.16 Affiliates are prohibited from sharing access cards to the building with others.

8.2.17 External parties responsible for support services are granted restricted access to important and sensitive areas only when necessary, and this access is closely monitored.

8.3 Visitor Access Controls:

8.3.1 Ideally, all sensitive IAU sites should have security checkpoints (where feasible) located at the reception area, staffed by security personnel. Visitors should only be allowed entry after registering in the visitor log, verifying their entry permit, and specifying the purpose of their visit.

8.3.2 Reception staff must make contact and obtain approval from the person the visitor intends to meet before granting them entry.

8.3.3 All visitors must be escorted in sensitive areas within the IAU site until the purpose of the visit is fulfilled. They should also be escorted until they exit the IAU facilities.

8.3.4 All visitors must wear visitor access cards at all times within the buildings, and any violation of this rule should be reported.

8.3.5 All visitors and individuals without clear identification cards should be stopped.

8.3.6 Visitors should not be allowed access to IAU devices or any other information processing assets without prior authorization.

8.3.7 Information about IAU visitors should be recorded upon reception in a "Visitor Log" and retained for periodic review. The log should include, but not be limited to, the following information:

- Visitor's name
- Visitor's identification
- Name of the visitor's affiliated IAU
- Purpose of the visit
- Name of the person the visitor intends to meet and their contact number.
- Entry time
- Exit time
- Visit date

8.4 Securing Workspaces:

8.4.1 All critical and sensitive areas must be consistently secured, such as data centres, server rooms, generator rooms, backup power sources, electrical rooms, air handling units, archival rooms, and areas where sensitive information is processed. Visitors should not be allowed access to these areas without necessary approvals from authorized personnel.

8.4.2 To secure facilities, rooms, and offices, the Security and Safety Management should consider the following security measures:

- Incorporating relevant health and safety regulations.
- Identifying locations of critical and sensitive areas or main facilities to prevent public access.
- Buildings and IAU facilities should have symbolic identification indicating their purpose, and clear signs should not be placed either inside or outside the building indicating information processing activities in these facilities.

- Preventing the public from accessing internal phone directories that identify locations of sensitive information processing facilities.
- Placing signs that read "Authorized Personnel Only" or "Restricted Access" at all entrances to critical and sensitive areas.
- Implementing officially documented safety and physical security procedures for working in critical and sensitive areas and adhering to them.
- Locking office spaces after working hours or when not in use.
- Installing intrusion detection alarm systems at designated locations to cover exterior doors, accessible windows, and other building entrances.

8.5 Protection from Environmental and External Threats:

8.5.1 User access to the IAU's data should be authorized, documented, and managed by application managers whenever possible. The process of granting/cancelling permissions should be monitored and recorded.

8.5.2 Temperature and humidity levels within critical and sensitive areas should be monitored to identify conditions that might negatively impact equipment operation, and corrective measures should be taken.

8.5.3 Critical and sensitive areas occupied by affiliates should be equipped with automatic emergency lighting that activates during power outages to facilitate evacuation during emergencies.

8.5.4 Hazardous or flammable materials should not be stored near information and technology assets, as they could pose threats or endanger these assets. Removable backup media should be stored in fire-resistant cabinets.

8.5.5 The university or building owner should provide fire detection and suppression systems, air conditioning systems, humidity control devices, and other environmental protection systems.

8.5.6 The Security and Safety Management should ensure that affiliates are adequately trained to use fire-fighting equipment, and regular building evacuation drills should be conducted.

8.5.7 Fire suppression equipment (fire extinguishers, fire blankets, self-extinguishing balls) should be provided throughout the university in sufficient numbers and appropriately distributed for easy access.

8.5.8 Smoke detectors should be present on all floors of office areas and inside server rooms, automatically triggering an alert upon smoke detection.

8.5.9 The Security and Safety Management should conduct regular inspections of fire safety equipment according to manufacturer's instructions or coordination with the building owner, and the equipment custodian should maintain maintenance records.

8.5.10 Additional preventative measures should be considered, as needed, to safeguard against threats such as floods, earthquakes, civil disturbances, and other natural or human-made disasters.

8.5.11 Environmental controls should be considered when defining controls, and relevant health and safety regulations should be taken into account, also considering security threats faced by neighbouring buildings.

8.5.12 The Security and Safety Management should ensure the following:

- Information processing facilities should not be located in an unstable environmental area.
- Information processing facilities should not be located near any hazardous neighbouring facilities (such as chemical labs).
- Installed fire detection and suppression devices should meet specified requirements from manufacturers.
- Alternative equipment and backup media should be stored at a safe distance from the main site to avoid exposure to the same disaster affecting the main site.

8.6 Equipment Security:

8.6.1 The DICT should ensure the following:

- All components of production systems in the university (e.g., servers, firewalls, routers) should be located within secure areas such as data centres or server rooms.
- All IP addresses of data processing assets should be treated as confidential and not disclosed to unauthorized individuals.

8.6.2 Alternative equipment or backup devices should be stored in locked secure areas, and locking mechanisms should be used to protect these resources when they are not in use during or after working hours.

8.6.3 Lightning arresters should be installed on all buildings housing sensitive information processing facilities and communication facilities (if possible).

8.6.4 Equipment locations should be identified to reduce unnecessary access to work areas.

8.6.5 Materials requiring special protection should be isolated to reduce the overall level of necessary protection.

8.6.6 Equipment processing sensitive information should be safeguarded to reduce the risk of information leaks.

8.6.7 Environmental conditions should be monitored to identify factors that could negatively impact the security of information processing operations.

8.6.8 Information processing facilities for the university should be designated to limit the risk of unauthorized individuals reviewing information during its use.

8.6.9 Facilities processing sensitive data should be isolated to apply additional controls.

8.6.10 Liquids and hazardous materials should be prevented from entering sensitive areas belonging to the university (e.g., data centres, recovery centres, information processing areas, monitoring centres, network communication rooms).

8.6.11 All environmental conditions affecting the operation of facilities processing sensitive information (e.g., temperature, humidity) should be monitored.

8.6.12 Necessary controls should be adopted to mitigate the risks of potential physical threats.

8.7 Supporting Facilities:

8.7.1 Security and safety management should ensure the following:

- All supporting facilities (such as electricity, water supply, heating, ventilation, and air conditioning) should be suitable for the systems they support.
- Regular inspections of supporting facilities should be conducted to ensure they are functioning as required, with appropriate records kept.
- Facilitate information processing facilities that manage sensitive operations through backup power sources to ensure continuous operation.

- Facilitate information processing facilities by placing power shutdown switches near emergency exits to facilitate rapid power reduction in case of emergencies.

8.8 Cable Security:

8.8.1 Security and safety management, in collaboration with the DICT, should ensure the following:

- Electrical supplies and communication cables should be underground whenever possible, or adequately protected using alternative methods.
- Network cables should be protected from unauthorized interception or damage, for example by using pipes to shield the cables or by avoiding routes in public areas.
- Clearly label cables and equipment for easy identification, reducing processing errors such as unintentional repair of network cables.
- Control physical access to information system transmission lines to prevent eavesdropping, alteration during transmission, disruption, or manipulation.
- The IAU should, as needed and based on risk approach, use electromagnetic protection to safeguard cables.
- Security and safety management, in collaboration with DICT, should conduct technical scans and regular inspections to ensure unauthorized devices are not connected to cables.
- Protect communication cables and data networks from wiretapping.
- If efficiency and availability requirements are high, the IAU should utilize fibber optic cables to improve reliability, protection, and efficiency.
- Isolate electrical power cables sufficiently from data network cables to prevent interference.
- Isolate data network cables and protect them from unauthorized interception or damage by routing them through protected areas.
- Conceal data network facilities and electrical power cables.
- Control access to cable distribution panel rooms.

8.9 Equipment Maintenance:

8.9.1 The DICT should ensure the following:

- Maintain all information system infrastructure used for production according to recommended service intervals and specifications by the supplier. Only qualified and authorized maintenance personnel should perform repairs and services.
- Conduct comprehensive maintenance of the entire system, including regular replacement/rep air of damaged parts and systems.
- Establish a maintenance plan for all components of the information system and communicate it to stakeholders.
- Apply necessary controls before maintenance to prevent leakage of sensitive IAU information.
- Keep appropriate maintenance records and review them.
- Perform equipment maintenance only by authorized individuals.

8.10Security of Device Usage Outside the IAU:

8.10.1 Regardless of ownership, the use of any information processing devices outside the IAU must be authorized.

8.10.2 Follow manufacturer instructions to protect devices when used outside the IAU.

8.10.3 Authorized devices taken outside the IAU should meet the same standards as those used within and for the same purposes.

8.10.4 The DICT should maintain accurate and up-to-date records of all devices taken outside the IAU.

8.10.5 Cybersecurity management permission is required to transfer devices, information, or software outside the IAU.

8.10.6 Apply controls based on specific security risks, considering risks associated with working outside the IAU.

8.10.7 The asset owner must ensure proper measures are taken when placing devices outside the IAU in accordance with safety requirements for the asset.

8.10.8 Asset managers should ensure continued use of devices placed outside the IAU comply with approved security policies within the IAU.

8.10.9 Users should maintain security of mobile devices such as laptops, tablets, etc., by:

- Not leaving devices open, logged in, or running when not in use.
- Not leaving devices and media unattended in public areas or other insecure areas.
- Not leaving devices in the IAU or work area after official working hours without using security controls (e.g., locking devices in a designated secure area).
- Avoiding the use of open and untrusted Wi-Fi networks in public places.
- Packing mobile IT devices like laptops and mobile devices with carry-on luggage while traveling.
- Reporting device loss immediately to the cybersecurity management and DICT and following instructions provided by the cybersecurity management.

8.11Managing Removable Media and Handling:

8.11.1 Appropriate procedures must be established to ensure the security of removable media and the confidentiality of stored information.

8.11.2 If information is no longer needed, contents of removable media set for removal from the source must be irrecoverable through the following methods:

- Shredding/destruction of papers, CDs, and DVDs using shredding machines capable of destroying them.
- Destruction of removable media (hard drives, magnetic external storage media) through demagnetization.
- In the absence of a paper shredder or demagnetization device, media should be destroyed by breaking, burning, or otherwise rendering them irrecoverable.
- All external storage media should be stored in a secure environment.
- Usage of external storage media devices should be restricted, and any exceptions should be authorized by cybersecurity management. All exceptions must be documented and stored.

8.12Secure Device Disposal and Reuse:

8.12.1 Devices or computer systems containing storage media should not be disposed of or reused until all confidential data and licensed software have been securely removed or replaced.

8.12.2 When retrieving devices assigned to users (such as laptops or workstations), reuse should only be considered after appropriate reformatting of computer systems (hard drives).

8.12.3 Any request for device disposal must have a valid justification and be authorized by asset managers or department heads, while considering operational business requirements and legal obligations.

8.12.4 The DICT should ensure the secure removal or replacement of all confidential data and licensed software before making a final recommendation for device disposal.

8.12.5 Personnel responsible for device and equipment disposal should maintain sufficient records for:

- Device disposal requests.
- Cybersecurity management recommendations.
- Signed disposal authorization records from specific personnel within the management.

8.12.6 Personnel should be educated about physical security best practices, such as clean desk policy and screen locking, and ensure their compliance.

8.13Asset Removal and Physical Media Transfer Controls:

8.13.1 The security and safety management should establish appropriate controls to prevent unauthorized access, misuse, or damage during the transfer of physical media to locations outside the IAU's IAU.

8.13.2 To protect information assets or media being transferred between locations, the following guidelines should be defined:

- Designate authorized personnel responsible for moving any media and software applications from within the IAU's IAU to external locations.
- Maintain records of media movement, and affiliates should take adequate measures to ensure the security of the media during transfer to external locations.
- When physical copies of confidential information are taken from the IAU's IAU, they must not be left unattended in a vehicle, hotel room, restaurant, or any other location.

8.14Dealing with Transactions Outside of Official Working Hours:

8.14.1 When handling transactions outside of official working hours, the following steps and guidelines should be followed:

- Ensure that the transactions are intended for the university and are properly classified, including the outgoing number, date, and ensuring the date is current.
- Verify that the transaction is properly sealed, signed, and in good condition.
- Clearly sign the receipt log for the transactions and include the date and time of receipt.
- After receiving the transactions, reception staff should immediately deliver them to the office of the manager. This should be documented separately, indicating the time of delivery.
- If no one is present in the manager's office, the transactions should be secured in the designated safe and then the manager of the university should be contacted for further instructions. This action should be recorded in the transaction's action section.

9 Roles and Responsibilities:

The authority for issuing card controls, instructions for the reception, visitor management, and transaction handling lies within the scope of the General Manager's authorization for the IAU.

The Cybersecurity Management responsibilities:

9.1.1 The Head of the Cybersecurity Management is responsible for approving the policy and ensuring its implementation.

9.1.2 The Head of the Cybersecurity Management shall approve the standards, procedures, and guidelines to ensure necessary compliance with security requirements for the IAU's operations.

9.1.3 The Head of the Cybersecurity Management is responsible for ensuring alignment between this policy and the IAU's operations.

9.1.4 The Head of the Cybersecurity Management is responsible for resolving any conflicts arising from this policy.

9.1.5 The Head of the Cybersecurity Management is responsible for providing the necessary resources to identify, acquire, and implement technical solutions to meet policy requirements, where feasible.

9.1.6 The Cybersecurity Management is responsible for disseminating this policy to all departments, affiliates, authorized users, or those who will be granted access to technical and information assets.

9.1.7 The Cybersecurity Management is responsible for coordinating with relevant departments to monitor compliance and execution.

9.1.8 The Cybersecurity Management is responsible for periodically reviewing the policy according to the established schedule.

The Security and Safety Management Responsibilities:

9.1.9 The Head of Cybersecurity Management shall have the authority and primary responsibility for physical and environmental security, as well as for awareness, training, and assessments.

9.1.10 Security and Safety Management shall Provide recommendations to support the identification, securing, and deployment of technical solutions to implement the requirements of the physical and environmental security policy whenever possible.

9.1.11 Security and Safety Management shall Guide the personnel within the university on the implementation and adherence to this policy.

9.1.12 The Head of Cybersecurity Management must adhere to this policy, implement the controls specified in this policy, and report any security incidents to the Head of the Cybersecurity Management.

Top Management, Heads of Departments, Heads of Units, and Advisers shall:

9.1.13 Ensure that this policy is shared with all affiliates within the university or department.

9.1.14 . Report any violations or non-compliance with this policy to the Cybersecurity Department Management.

9.1.15 Ensure that all affiliates within IAU shall adhere to the provisions of this policy and report any security incidents or non-compliance with any provisions outlined in this policy to the Head of the Cybersecurity Management.

10 Ownership of the Policy:

The person responsible for this policy is the Head of the Cybersecurity Management within the IAU.

11 Changes to the Policy:

The policy should be reviewed at least annually or when there are changes in legislative and regulatory requirements. Changes should be documented and approved by the authorized party within the IAU.

12 Compliance:

All affiliates within the IAU, as well as external parties/contractors, are required to comply with the provisions of this policy. The Head of the Cybersecurity Management within the university must ensure continuous monitoring of compliance and provide periodic reports to the authorized party.

Necessary actions must be taken to ensure compliance with the provisions of this policy. This can be achieved through periodic reviews conducted by the Cybersecurity Department or relevant departments. Corrective actions should be taken by the authorized party within the university based on recommendations provided by the Head of the Cybersecurity Management regarding any violations of this policy. Disciplinary actions should be proportionate to the severity of the incident, as determined by the investigation. Disciplinary actions may include, but are not limited to:

- Revoking access privileges to data, IT assets, and connected systems.
- Issuing a written warning or terminating the employment of the affiliate, as deemed appropriate by the IAU.

Non-compliance with any provisions of this policy - without prior approval from the Cybersecurity Department - should result in appropriate actions being taken in accordance with the IAU's policies and regulations, or as appropriate, and in line with contractual terms with individuals or entities contracted with the IAU.

13 Related Policies, standards and Procedures

- DICT.I.06-01.CS.E.V2.0 - General Cybersecurity Policy
- DICT.I.06-02.CS.E.V2.0 - Cybersecurity Compliance Policy
- DICT.I.06-21.CS.E.V2.0 - Data Classification Policy
- DICT.I.06-26.CS.E.V2.0 - Clean Desk and Screen Policy
- DICT.I.06-04.CS.E.V2.0 - Asset Management Policy
- DICT.I.06-27.CS.E.V2.0 - Acceptable Use of Assets Policy
- DICT.I.06-60.CS.E.V2.0 Asset Classification Standards
- DICT.I.06-62.CS.E.V2.0 Asset Management Standards

14 References

Department Name	National Institute of Standards and Technology (NIST)	ISO 27001:2013	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts of Entities	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Core Cybersecurity Controlsي
Physical Security Domain	PE-3, PE-4, PE-5	A.11.1.1	-	-	-	-	**3-14-2**
Physical Access Control	MA-5, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8	A.11.1.2	-	-	-	-	**3-14-2**
Visitor Entry	MA-5, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8	A.11.1.2	-	-	-	-	**3-14-2**
Facilities, Rooms, Important and Sensitive Offices	PE-3, PE-4, PE-5	A.11.1.3	-	-	-	-	**3-14-2**
Protection from Environmental and External Threats	CP-2, CP-6, CP-7, PE-1, PE-9, PE-13, PE-15, PE-18, PE-19	A.11.1.4	-	-	-	-	**3-14-2**
Working in Secure Areas		A.11.1.5					
Equipment Security - Equipment Installation and Protectionا	PE-13, PE-14, PE-15, PE-18, PE-19	A.11.2.1, A.11.2.6	-	-	-	-	**3-14-2**
Supporting Facilities	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14	A.11.2.2	-	-	-	-	**3-14-2**
Cable Security	PE-4, PE-9	A.11.2.3	-	-	-	-	**3-14-2**
Equipment Maintenance	MA-2, MA-3, MA-4, MA-5, MA-6	A.11.2.4	-	-	-	-	**3-14-2**
Security of Device Usage Outside the University	AC-19, AC-20, MP-5, PE-17	A.11.2.6	-	-	-	-	**3-14-2**

Secure Handling and Reuse of Devices	MP-6	A.11.2.7	-	-	-	-	**3-14-2**
Not Leaving Devices Unattended		A.11.2.8					
Removable Media Management	MA-2, MP-5, PE-16	A.8.3.1	-	-	-	-	**3-14-2**
Asset Disposal and Physical Media Transfer Controls	MA-2, MP-5, PE-16	A.8.3.3, A.11.2.5	-	-	-	-	**-**

--End of Document---