ICT SECURITY PROCEDURE

PREPARED FOR:

International Islamic University Malaysia

PREPARED BY:

Information Technology Division

Release Version	Date	Pages Affected	Remarks/Change Reference
Version 1.0	*16/12/2019*	-	Endorsement by ICT Committee
Version 2.0	*18/11/2024*	*The entire Policy page has been updated.*	The Policy change to Procedure

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Shahidah Mahbob	Endorsement by ICT Committee	12/12/2019	16/12/2019
Syed Mohd Hazrul Bin Syed Salim	Draft new ICT Security Policy and reviewed by OLA - advised to change to Procedure	18/11/2024	-
Shahidah Mahbob	ICT Security Policy updated to ICT Security Procedure	18/12/2024	-
Shahidah Mahbob	The ICT Security Procedure reviewed by SIRIM Consultant	14/01/2025	27/03/2025
Shahidah Mahbob	Recommended through ITD Management Meeting No. 6	14/04/2025	16/04/2025
Shahidah Mahbob	Reviewed by ICT Committee Members	15/07/2025	
Shahidah Mahbob	Reviewed by ITD Senior Management Members	22/09/2025	
Shahidah Mahbob	Endorsement by ICT Committee (via circulation)		

ARTICLE 1:

DEVELOPMENT AND MAINTENANCE PROCEDURE

ARTICLE 01 DEVELOPMENT AND MAINTENANCE PROCEDURE	
0101 ICT Security Procedure	
Objective: To explain the direction and management support for information security in accordance with IIUM vision and mission.	
IIUM-010101 Procedure Implementation	
Implementation of this Procedure will be carried out by the Rector assisted by the ISMS Steering Committee.	
IIUM-010102 Procedure Dissemination and Use	
This Procedure is to be disseminated and is applicable to all users of IIUM ICT assets.	ITD Management

IIUM-010103 Procedure Maintenance	
The IIUM ICT Security Procedure is subject to revisions and amendments based on scheduled revision in line with the changes in technology, applications, procedures, legal requirement and government circular and policies. The following is the procedure to be followed in relation to the revision of IIUM ICT Security Procedure: (a) Identify and define the necessary amendments; (b) Submit the recommended revised Procedure to the ICT Committee for endorsement; (c) Submit to the Board of Governance for approval and implementation; (d) Changes to the approved Procedure shall be disseminated to the IIUM community, and all parties related to ICT services; and (e) This Procedure shall be reviewed as required to adapt to current needs, ensuring that documents remain relevant.	ITD Management, Document Controller
IIUM-010104 Procedure Applicability	
The IIUM ICT Security Procedure is applicable to all users of any IIUM ICT assets without exemption.	~~All~~ All Staff All Student

ARTICLE 2: ICT SECURITY ORGANIZATION

ARTICLE 02 ICT SECURITY ORGANIZATION	
0201 Internal Organizational Infrastructure	
Objective: To describe the roles and responsibilities of the individuals involved clearly and systematically to achieve the IIUM ICT Security Procedure objectives.	
IIUM-020101 Rector	
The Rector has roles and responsibilities in matters such as the following: (a) Ensure the enforcement of the Procedure implementation; (b) Ensure that all users understand and comply to the IIUM ICT Security Procedure; (c) Ensure adequate budget and resources are allocated to support ICT security initiatives, which includes staffing requirement and development, and adequate cybersecurity protections (awareness, training, cybersecurity equipment and infrastructure) in the University; (d) Ensure risk management and cybersecurity initiatives for the University is implemented as required by the Procedure; and (e) Appoint CD/IO.	Rector

IIUM-020102 Chief Digital/Information Officer (CD/IO)	
The CD/IO's roles and responsibilities are as follows: (a) Assist the Rector in the implementation of IIUM ICT Security initiatives; (b) Ensure the implementation of ICT security controls within the service delivery system of the University; (c) Ensure the ICT security controls are incorporated in the University's ICT strategic planning; (d) Oversee the implementation and coordination of training plans and ICT security awareness programs; (e) Formulate and plan risk management and audit related to cybersecurity; (f) Responsible for communicating ICT security incidents to the University management; (g) Oversee the development and implementation of IIUM ICT security procedures and guidelines to ensure align with best practices and legal/regulatory requirements; and (h) The IIUM Chief Digital/Information Officer's roles and responsibilities as defined in ICT Regulations.	CD/IO
IIUM-020103 ITD Director	
The roles and responsibilities of ITD Director in ensuring the implementation of the Procedure in all IT initiatives and operations are as follows: (a) Enforce the ICT Security Procedure in the University; (b) Coordinate ICT security program for the University; (c) Ensure implementation access controls for all users of IIUM ICT assets;	ITD Director

(d) Ensure proper records of evidence and reports on ICT security threats; (e) Ensure confidentiality, integrity and availability of information within or outside the IIUM; (f) A member of the ICT Committee; and (g) Appoint ICTSO.	
IIUM-020104 ICT Security Officer	
Roles and responsibilities ICT Security Officer appointed are as follows: (a) Enforce the IIUM ICT Security Procedure to all users in the University; (b) Establish and review guidelines and procedures in accordance with the IIUM ICT Security Procedure; (c) Coordinate and oversee the comprehensive IIUM ICT security initiatives; (d) Implement the cybersecurity controls/action plan addressed in risk management for cybersecurity; (e) Implement cybersecurity audits based on the cybersecurity controls/action plan; (f) Issue alerts to the IIUM campus community regarding potential threats like viruses, and provide advice on protective measures; (g) Disseminate information and raise awareness about the IIUM ICT Security Procedure to all users; (h) Report on ICT security incidents to the IIUM ICT Computer Security Incident Response Team (CSIRT) and inform the ITD Management, ITD Director and the CD/IO;	ICTSO

(i) Report any ICT security-related matters or discoveries to the ITD Management; (j) Collaborate with relevant parties to identify the source of threats or security incidents and promptly implement ICT remedial measures; and (k) Plan and implement cybersecurity trainings and awareness programs.	
IIUM-020105 ICT System Administrator	
IIUM ICT Systems Administrators include all Heads of Sections in the Information Technology Division (ITD), IIUM, as well as the Head of the IT Department at Sultan Ahmad Shah Medical Centre. The roles and responsibilities of the ICT system administrators are as follows: (a) Take appropriate actions immediately upon being informed of staff resignations, transfers, extended leave, lengthy courses, changes in job scopes, or changes in the academic status of students, as well as any relevant changes involving third parties. (b) Monitor daily access activities of user applications; (c) Identify abnormal activities such as unauthorized data breaches and alterations, and cancel or stop the activities immediately; (d) Analyse, review and keep audit trail records; and (e) Provide a report on access activities on a regular basis;	ICT System Administrators

IIUM-020106 University Technical ICT Sub- Committee	
The function of UTICTEC as described in ICT Regulations which includes planning and determine the measures/steps for cybersecurity.	UTICTEC
IIUM-020107 ISMS Steering Committee	
The roles and responsibilities of the ISMS Steering Committee are as follows: (a) Plan resource requirements related to the ISMS activities; (b) Monitor the effectiveness of the ISMS implementation periodically; (c) Approve any proposed documentation; (d) Make any amendments to the ISMS scope of the Procedure; (e) Review and verify reports from ISMS Task; (f) Recommend implementation of ISMS awareness and training; (g) Review the ISMS scope; (h) Review the criteria of risk acceptance, level of risk and risk treatment plan; and (i) Prepare the procedure for internal audit.	ISMS Steering Committee
IIUM-020109 Users	
The roles and responsibilities of Users are as follows: (a) Read, understand and comply with IIUM ICT Security Procedure;	~~User~~ All Users

(b) Users need to be aware of and understand the implications of ICT security in relation to one's actions;

(c) Users need to undergo security screening if required to deal with classified official information;

(d) Users need to implement the principles of the IIUM ICT Security Procedure and maintain the confidentiality of IIUM information;

(e) Users need to report any ICT security-threatening activities to the ICT Security Officer (ICTSO) immediately;

(f) Users need to participate in awareness programs on ICT security;

(g) Users need to sign the Compliance Declaration for IIUM ICT Security Procedure as per **Appendix 1;**

(h) Users need to maintain the confidentiality of cyber security controls from public knowledge; and

(i) Users need to implement protective measures while handling ICT resources as follows:

i) Users need to prevent disclosure of information to unauthorized parties;

ii) Users need to check the information and determining that it is accurate and complete from time to time;

iii) Users need to determine the information ready for use;

iv) Users need to maintain confidentiality of information;

v) Users need to comply with established government cyber security act, standards and guidelines;

vi) Users need to implement regulations related to classified information especially during creation, processing, storage, transmission, delivery, exchange and destruction;

IIUM-020110 IIUM ICT Computer Emergency Response Team (CSIRT)	
The roles and responsibilities of CSIRT are as follows: (a) Receive and detect ICT security complaints and assess the level and types of incidents; (b) Record and conduct initial investigations of received incidents; (c) Act on ICT security incidents reported; (d) Handle ICT security incident responses and take minimum recovery actions; (e) Advise the related KCDIOM to take recovery and fortification action if the incident that occurred involves ICT assets that are under the responsibility of the KCDIOM; (f) Contact and report the incident to NACSA; (g) Prepare incident handling reports for the consumption of the University authority~~;~~ (h) Provide advisory services to users in locating, identifying and handling of any ICT security incidents; (i) Disseminate information to assist in the strengthening of ICT security in IIUM from time to time; and (j) Conduct assessments and evaluations to verify that the existing ICT security measures are sufficient and take remedial	CSIRT

or strengthening action to increase the level of ICT infrastructure security so that new incidents can be avoided.	
0202 Third Parties	
Objective: Ensure the security of all ICT assets used by third parties (vendors, consultants, and others).	ICT System Administrators
IIUM-020201 Requirements of Contract with the Third Parties	
This is to ensure that the use of information and information processing facilities by third parties are controlled. Matters that need to be complied with are as follows: (a) Read, understand and comply with the IIUM ICT Security Procedure; (b) Identify information security risks and information processing facilities and implement appropriate controls before granting access permissions; (c) Identify security requirements before granting access or use to third parties; (d) Access to IIUM's ICT assets needs to be based on a contractual agreement; (e) Ensure that all security requirements are clearly specified in agreements with third parties. The following items should be included in the agreement: i. Compliance Declaration for IIUM ICT Security Procedure;	ITD Management, ICT System Administrators and Third Parties

ARTICLE 3: ASSET MANAGEMENT

ARTICLE 03

ASSET MANAGEMENT

0301 Responsibility for Assets

Objective:

To determine all ICT assets and provide the appropriate control and protection for the assets.

IIUM-030101 ICT Asset Inventory

Ensure that all ICT assets are given the appropriate control and protection by the owner or respective asset custodian. The following statements shall be adhered to: (a) All ICT assets must undergo proper identification and documentation. Asset information must be recorded and constantly updated; (b) Ensure that each ICT asset has designated owners. Access and operation of ICT assets are exclusively granted to authorized users based on their defined roles, responsibilities or specific access rights; (c) Asset owner must confirm the physical location of ICT assets within IIUM to facilitate the monitoring and tracking of asset movements; (d) Identify, document and enact a set of rules for the proper handling of ICT assets across IIUM; and (e) Users are accountable for the assets and must follow the University's policies and guidelines for asset management and security.	Finance Division KCDIOM Asset Liaison Officer and All Staff

0302 Information Classification and Handling	
Objective: Ensure all information or ICT assets are given the appropriate level of protection	
IIUM-030201 Information Classification	
Information should be classified and labelled accordingly. Every classified information must have a security level in accordance with the Guideline on Information Classification and Labelling.	OSIC
IIUM-030202 Information Handling	
Information handling activities such as collecting, processing, storing, sending, conveying, changing and destroying must consider the following security measures: (a) Prevent disclosure of information to unauthorized parties including Artificial intelligence (AI) tool; (b) Checking information and determining it is accurate and complete from time to time; (c) Ensure the information is ready for use; (d) Maintain password confidentiality; (e) Complying with established safety standards, procedures, measures and guidelines; (f) Paying attention to classified and personally identifiable information especially during creating, processing, storing, delivering, exchanging and destroying information;	Finance Division, KCDIOM Asset Liaison Officer, ICT System Administrators, All Staff

(g) Keeping ICT security measures confidential from the public; and (h) Ensuring any unused data shall be deleted according to the Guideline for Information Classification. (i) Ensuring any use of AI tools according to the University Procedure and Guidelines.	
IIUM-030203 Hardware Disposal	
Obsolete and beyond economic repair of IT assets and inventory supply by IIUM shall be disposed. ICT equipment must be disposed of through the existing University disposal procedures. The disposal should be conducted in IIUM controlled and comprehensive manner. The following statements shall be adhered to: (a) All data/content on the equipment must be securely erased prior to disposal; (b) The user shall be responsible for making a backup copy of data prior to the disposal exercise; (c) The data stored in ICT equipment to be disposed of must be securely erased in a safe manner before transfer or disposal, ensuring that it is completely written off to prevent any data recovery or unauthorized access; (d) Assets Liaison Officer shall identify equipment to be disposed;	ITD Management, ICT System Administrators, ITD Staff, Asset Liaison Officer

(e) Equipment to be disposed shall be kept at the place designated with security features to ensure the safety of the equipment; (f) The Asset Liaison Officer is responsible for recording the disposal details and update the disposal records of ICT equipment; (g) Compliance with Guideline for Disposal of ICT Resources; (h) The user is STRICTLY PROHIBITED from doing the following: i. Retain any of ICT equipment to be disposed for personal use; ii. Disconnect, dismantle and store additional CPU internal devices such as RAM, hard-disk, motherboard and so forth; iii. Store or transfer external computer hardware such as speakers and any related equipment to any part of IIUM; iv. Moving any hardware that is to be disposed out of IIUM; v. Self-disposing the ICT equipment;	

ARTICLE 4: HUMAN RESOURCE SECURITY

ARTICLE 04

HUMAN RESOURCES SECURITY

0401 Human Resources Safety in Daily Activities

Objective:

To clearly define the responsibilities and implement the necessary measures to ensure that all personnel with access to IIUM's ICT resources consistently maintain the highest standards of security.

IIUM-040101 Before Employment / Before the Service

The following statements shall be adhered to: (a) Collaborate with relevant departments to clearly define the roles and responsibilities of IIUM staff and individuals involved in IIUM's ICT services, ensuring ICT asset security before, during, and after service engagement. (b) Conduct security screening for IIUM personnel, vendors, consultants, and individuals involved in IIUM's ICT services based on applicable legal, regulatory, and ethical requirements that align with service needs, the level of information accessed, and anticipated risks; and ensure compliance with service agreements prior to commencement. (c) Ensure that all IIUM personnel and external parties comply with the terms, conditions, and regulations specified in service agreements prior to the commencement of service. (d) Provide an orientation session covering IIUM's ICT policies, security protocols, and responsibilities. (e) Ensure completion of all required documentation, including contracts and confidentiality agreements.	MSD

(f) Coordinate with IT team to provide necessary ICT access and equipment. (g) Facilitate initial training on IIUM's ICT systems and security practices. (h) Collaborate with relevant departments to clearly define the roles and responsibilities of third-party service providers involved in IIUM's ICT services, ensuring ICT asset security before, during, and after service engagement. (i) Facilitate and oversee comprehensive security screenings for all third-party service providers, ensuring alignment with legal, regulatory, and ethical standards, as well as service needs, access levels, and potential risks. (j) Ensure that all third-party service providers comply with the terms, conditions, and regulations specified in service agreements prior to the commencement of service. (k) Ensure that Third-Party Service Providers within their units are aware of and comply with security screenings and role definitions. (l) Comply with the security requirements and role definitions provided by the respective Kulliyyah/Center/Institute/ Division/Office/Mahallah, ensuring completion of all necessary security screenings before commencing service. (m) Follow the roles and responsibilities as defined by MSD and their respective units, ensuring compliance with all security screenings and service agreements before starting service.	KCDIOM Third-Party Service Providers All Staff

IIUM-040102 During Service	
The following statements shall be adhered to:	
(a) Coordinate and provide ongoing education and training on IIUM ICT Security Policy, the Information Security Management System (ISMS), and relevant security-related products, functions, applications, and systems.	MSD
(b) Oversee the enforcement of disciplinary procedures and/or by-laws for non-compliance with IIUM's established laws and regulations, in collaboration with relevant departments.	
(c) Ensure that staff and Third-Party Service Providers manage ICT assets securely, adhering to IIUM's legislation and regulations.	ITD
(d) Promote awareness and understanding of ICT applications among users, ensuring proper utilization while emphasizing the importance of ICT security.	
(e) Monitor and ensure that all staff, Third-Party Service Providers, and other relevant parties within their units adhere to ICT security procedures and regulations, participating in training provided by MSD and ITD.	KCDIOM
(f) Report any non-compliance or security incidents to MSD and ITD for immediate action and resolution.	
(g) Manage ICT assets securely in accordance with IIUM's policies and regulations, actively participating in required training provided by MSD and ITD.	Third-Party Service Provider
(h) Manage ICT assets responsibly, in line with IIUM's policies, and engage in continuous learning and technical training coordinated by MSD to effectively fulfil their duties.	All Staff

IIUM-040103 Change or End of Service	
IIUM personnel who have ended their service should comply with the following:	
(a) Ensure the return of all ICT assets from departing staff and other individuals in accordance with established regulations and service terms.	MSD
(b) Coordinate with ITD to revoke all access permissions and retrieve ICT equipment	ITD
(c) Ensure that all offboarding documentation, including the return of access cards and equipment, is completed.	
(d) Verify that all confidentiality agreements and service obligations are fulfilled before finalizing the departure process	
(e) Revoke all access permissions to information and information processing facilities for personnel and Third-Party Service Providers whose service has ended, in line with IIUM's regulations.	ITD
(f) Delete all official IIUM information from the devices of third-party service providers and departing staff.	
(g) Ensure that all departing personnel and Third-Party Service Providers within their units return ICT assets and that access permissions are revoked, coordinating with MSD and ITD.	KCDIOM
(h) Ensure that all official IIUM information is securely removed from the devices of third-party service providers and departing staff.	
(i) Return all ICT assets to IIUM and ensure that no official information is stored on personal devices or taken offsite, in strict compliance with IIUM regulations.	Third-Party Service Providers, All Staff

ARTICLE 5: PHYSICAL AND ENVIRONMENT SECURITY

ARTICLE 05

PHYSICAL AND ENVIRONMENTAL SECURITY

0501 Area Security

Objective:

To prevent unauthorized physical access that could lead to theft, damage, or disruption to information and IIUM's information processing facilities.

IIUM-050101 Areas of Control

This aims to prevent unauthorized access, physical interference, and damage to the premises and ICT assets of IIUM. The following statements shall be adhered to: (a) The area of physical security should be clearly identified. Location and the strength of physical security must rely on the need to protect assets and revenue risk assessment; (b) Use perimeter security (barriers such as walls, fences, controls, security guards, etc.) to protect areas containing information and information processing facilities; (c) Protect restricted areas through appropriate entrance controls to ensure that only authorized personnel can access these entry points; (d) Design and implement physical security within offices, rooms, and facilities;	OSEM, Development Division, CD/IO, ITD and KCDIOM

(e) Design and implement physical protection from fire, floods, explosions, human interference, and any natural or human-made disasters; (f) Implement physical protection and provide guidelines for staff working in restricted areas; (g) Install security alarms or cameras; (h) Provide a safe or a special area for visitors; (i) Establish a Security Control Services; (j) Protect the limited area by appropriate entry controls to ensure that only authorized personnel can pass through this gateway; (k) Design and implement physical security in the office, room and facilities;	

IIUM-050102 Physical Entry Control	
The following statements shall be adhered to: (a) Every IIUM staff and student must be able to display their University ID while on campus; (b) All University ID must be handed back to the University when the user resigns or retires; (c) Using passwords to access a computer system is required; (d) All ICT equipment must be protected from theft, damage, abuse or unauthorized modifications; (e) All critical equipment must be placed in an area with appropriate temperature control; air-conditioned and ventilated; (f) The critical equipment must be supported by the Uninterruptable Power Supply (UPS); (g) All ICT equipment shall be stored or placed in an organized, clean location with security features. Networking equipment, such as switches, hubs, routers, etc., should be placed inside the specified racks and in a secured area; (h) Removal of ICT equipment from IIUM premises must be approved by Deans or Directors and be recorded for monitoring purposes; (i) The loss of ICT equipment should be immediately reported to ITD and the Assets Liaison Officer of the KCDIOM;	All Users Head of KCDIOM

(j) Users are not allowed to move any ICT equipment from its original location without the permission of ITD and the Assets Liaison Officer of the KCDIOM;

(k) Any damages of the ICT equipment must be reported to ITD to be repaired;

(l) Any stickers other than those intended for official purposes (asset tags) are not allowed. This is to ensure that equipment remains in pristine condition;

(m) IP address configuration is not allowed to be modified from the original IP address;

(n) Users are strictly forbidden from changing administrator password set by ITD;

(o) Users are responsible for the hardware, software and information under their supervision, and these shall be used for official work only;

(p) Any form of fraud or misuse of the ICT equipment shall be reported to ITD;

(q) Ensure that the plug is disconnected from the main switch (main switch) to prevent hardware breakdown before leaving the office in events such as thunder, lightning, etc.;

(r) Visitors must register and obtain a visitor security pass at the OSEM and must return it after the visit;

(s) Loss of University ID and passes must be reported immediately to OSEM; and (t) Only authorized users can use IIUM's ICT assets.	
IIUM-050103 Protected Areas	
A protected area is defined as an area which is restricted to certain officers only. It is implemented to protect ICT assets available in the area. Protected areas in IIUM are listed in **Appendix 2.** (List of Protected Areas in IIUM) The following statements shall be adhered to: (a) Access to restricted areas is limited to only authorized officers; and; (b) All third parties are prohibited from entering restricted areas except in certain cases such as when providing support services or technical assistance, and they must be accompanied by the authorized person at all times until the task is completed in the area.	ICT System Administrators
0502 Equipment Security	
Objective: Protect IIUM ICT equipment from loss, damage, theft as well as interference with the equipment.	

IIUM-050201 ICT Equipment	
The following statements shall be adhered to: (a) Users should check and ensure that all ICT equipment under their control functions properly; (b) Users are solely responsible for their own computers and are not allowed to make any changes in hardware and configurations that have been set; (c) Users are strictly forbidden to add, disassemble or replace any specified ICT hardware; (d) Users shall not make any additional software installation without permission from ICT System Administrator (for the equipment provided by the University); (e) Users are responsible for damage or loss of ICT equipment under their control; and (f) Users must ensure that the antivirus software in their personal computers is always activated and updated as well as perform scans on the storage media used;	All Staff

IIUM-050202 Storage Media	
The following statements shall be adhered to: (a) The storage media should be kept in an appropriate storage space with the relevant security features in accordance with its informational content; (b) Entry access to the media storage areas shall be limited to authorized users only; (c) All storage media must be controlled to prevent unauthorized access, theft, and destruction; (d) All storage media containing critical data must be stored in a safe with security features including resistance to break-downs, fire, water and magnetic fields; (e) Access and movement of the storage media should be recorded; (f) The physical devices used for data backup should be managed and maintained within a specific, secure location. (g) To provide a copy or replication (backup) on a second storage media for the security purposes and to prevent loss of data; (h) All storage media to be retired must be destroyed properly and securely; and (i) Approval from the owner must be obtained prior to the deletion of critical data or media content.	All Staff

IIUM-050203 Electronic Signature Media	
The following statements shall be adhered to: (a) The user shall be solely responsible for the media of the electronic signatures to protect against theft, loss, damage, abuse and replication; (b) Media cannot be transferred or loaned; and (c) Any incidents of media loss incurred should be immediately reported to ICTSO for further action.	All Staff
IIUM-050204 Software Media and Applications	
The following statements shall be adhered to: (a) Only licensed software is approved for use at IIUM; (b) IIUM in-house applications are not allowed to be demonstrated or distributed to other parties except with the consent of the ITD Management; (c) Software Licenses (registration code, serials, CD keys) must be kept separate from the CD-ROM, disk, or related media to prevent the occurrence of theft or piracy; (d) System source code should be stored properly, and any modifications must be in accordance with established procedures; and (e) Comply to the Policy of Responsible Use of ICT Resources for IIUM Staff and Student.	All Staff

IIUM-050205 Hardware Maintenance	
Hardware must be properly maintained to ensure its availability, confidentiality, and integrity. The following statements shall be adhered to: (a) All hardware must be maintained as defined by the manufacturer; (b) Ensure that the hardware will only be maintained by authorized personnel or parties only; (c) Examine and test all the hardware before and after the maintenance process; (d) Inform the user before performing the maintenance.	ICT System Administrators, ITD Team Leaders
IIUM-050206 The Equipment Outside Premises	
The following statements shall be adhered to: (a) Equipment must be protected at all times; and (b) The storage or placement of equipment must incorporate suitable security features.	~~All User~~ All Users
0503 Environmental Safety	
Objective: Prevent IIUM ICT assets from any form of environmental threat caused by natural disasters, errors, negligence, or accidents.	

IIUM-050301 Environmental Control	
The following statements shall be adhered to: (a) Thoroughly plan and prepare an overall layout plan of the data center, (b) All office spaces particularly areas with ICT facilities should be equipped with adequate and authorized security protection such as firefighting equipment and emergency exits; (c) Protective equipment must be installed in the right places, easily recognized and handled; (d) Flammable materials must be stored at the designated location; (e) All liquid substances must be placed in the designated location and distanced from the ICT asset; (f) Users are prohibited from smoking or using cooking utensils such as electric kettles near the computer equipment; (g) All protective equipment shall be checked and tested in accordance with the manufacturer's manual. Activities involved in and the results of this test should be recorded for ease of reference and action if necessary; and (h) Access to the riser vessel must always be locked.	ITD, OSHBE, Appointed Service Provider, Development Division

IIUM-050302 Power Supply	
The following statements shall be adhered to: (a) All critical equipment must be protected from power failures and appropriate power supplies should be channeled to the ICT equipment; (b) Equipment supports such as Uninterruptable Power Supply (UPS) and generators can be used for critical services such as data center to get constant power supply; and (c) All power supply supporting equipment must be checked and tested regularly.	ITD, Appointed Service Provider, Development Division
IIUM-050302 Cables	
The following statements shall be adhered to: (a) Using cables in accordance with the defined specifications; (b) To protect the cables from intentional or unintentional damage; (c) Protect the cable installation route completely to avoid the threat of damage and wiretapping; and (d) All cables must be clearly labeled and must be through a cable trunking to ensure the safety of cable from damage and information interception.	ITD, Development Division

IIUM-050304 Emergency Procedures	
The following statements shall be adhered to: (a) Each user must read, understand and comply with emergency procedures with reference to IIUM HSE Emergency Preparedness and Response: IIUM-HSE-PROC-08; and (b) Any emergency such as fire shall be reported to OSEM as IIUM ERT Campus level.	All Users, OSHBE, OSEM
0504 Document Security	
Objective: To protect IIUM information from any form of environmental threats caused by any form of natural disasters, accidents or negligence.	
IIUM-050401 Documents	
The following statements shall be adhered to: (a) Each document shall be filed and labeled in accordance with Guideline for Information Classification and Labelling; (b) Movement of files and documents should be recorded and must follow related procedures; (c) Loss and damage of all types of documents need to be notified in accordance with related procedure; (d) Disposal of documents should be performed in accordance with current safety procedures and the procedures of the National Archives; and (e) Using encryption on the official secret documents prepared and transmitted electronically.	All Staff

ARTICLE 6: OPERATIONS MANAGEMENT AND COMMUNICATIONS

ARTICLE 06 OPERATIONS MANAGEMENT AND COMMUNICATIONS	
0601 Operating Procedure Management	
Objective: Ensure secure and proper operation of services and information processing facility.	
IIUM-060101 Procedure Handling	
The following statements shall be adhered to: (a) All established ICT procedures must be identified, documented, stored, and controlled; (b) Each procedure must include clear, systematic, and comprehensive instructions, (c) All procedures must be periodically updated or as needed; and (d) All IIUM personnel must adhere to the established procedures.	All Staff
IIUM-060102 Change Management	
The Change Management process must be adhered to the Procedure on Management of IT Change.	All Staff

IIUM-060103 Segregation of Duties and Responsibilities	
The following statements shall be adhered to: (a) The duties and responsibilities should be segregated to reduce the likelihood of misuse or unauthorized modifications to ICT assets; (b) Tasks involving the creation, deletion, updating, modification, and verification of data should be separated to prevent unauthorized access and safeguard ICT assets from errors, limited information leaks, or manipulation; and (c) Tools and hardware used for development, updates, maintenance, and testing of applications should be segregated from the production environment.	ITD Director, ICT System Administrators, ITD Team Leaders

0602 Third-Party Management Delivery Services

Objective:

Ensure the implementation and maintenance of information security levels and the delivery of services including cloud services are in accordance with the service agreement with third parties and related policies.

IIUM-060201 Delivery of Service	
The following statements shall be adhered to: (a) Ensure the security, service terms, and delivery levels contained in the agreement are complied with, implemented, and maintained by third parties. (b) Services, reports, and records submitted by third parties need to be continually monitored, reviewed, and verified; and (c) Ensure compliance with the Guidelines of IIUM ICT Vendor Management.	ITD Management, ICT System Administrators
0603 System Planning and Acceptance	
Objective: Minimizing risks that may lead to system disruptions or failures.	
IIUM-060301 Capacity Planning	
The following statements shall be adhered to: (a) The capacity of any ICT component or system should be carefully designed, managed, and monitored by the respective personnel to ensure its adequacy and suitability for the development and use of ICT systems in the future; (b) These capacity requirements should also consider ICT security features to minimize risks such as service disruptions and losses due to unplanned modifications. (c) Compliance to the Procedure on Performance and Capacity Planning	ITD Management, ICT System Administrators

IIUM-060302 System Acceptance	
Ensure adherence to the procedure on Management of Quality Test and UAT.	ITD Management, ICT System Administrators
0604 Malicious Software	
Objective: Protecting the integrity of software and information from exposure or damage caused by malicious software such as viruses, Trojans and etc.	
IIUM-060401 Protection from Malicious Software	
The following statements shall be adhered to: (a) Install security systems to detect software or hazardous programs, such as antivirus, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS) following proper and secure usage procedures; (b) Install and use only genuine software, registered and protected under any enforcement written law; (c) Scan all software or systems with antivirus software before using them; (d) Keep antivirus programs updated with the latest virus definitions;	All Staff

(e) Periodically review the content of systems or information to detect unwanted activities such as loss and damage of information; (f) Participate in cybersecurity awareness programs on the threats of malicious software and how to handle them; (g) Include liability clauses in any contracts offered to software vendors. (h) Implement quality assurance programs and procedures on all developed software. (i) Issue warnings about ICT security threats such as virus attacks; and (j) Periodically review the logs of ICT security devices and advisories to analyze the patterns of attack from malicious software.	
IIUM-060402 Protection against Mobile Code	
The following statements shall be adhered to: (a) The use of mobile code, which can threaten ICT security, is not allowed.	IT Staff
0605 Housekeeping	
Objective: Protecting the integrity of information and communication services to ensure accessibility.	
IIUM-060501 Back-up	
To ensure that the system can be rebuilt after a disaster, back-up copies must be created each time configurations change. The back-up copies shall be recorded and stored off site.	ICT System Administrators, IT Staff

The following statements shall be adhered to: (a) Create backup copies of all software, applications and configuration which include after changing to new appliances, server and network devices at least once or after obtaining a new version; (b) Generate duplicate copies of all data and information as per operational needs. The frequency of duplication depends on the criticality of the information; (c) Test the backup system and existing restore procedures to ensure they function perfectly, are trustworthy, and effective when used, especially during emergencies; (d) Backups should be conducted daily, weekly, and monthly, depending on the information's criticality; and (e) Record and store backup copies in different secure locations.	

0606 Network Management

Objective:

Secure the information within the network and its supporting infrastructure.

IIUM-060601 Network Infrastructure Control	
To enhance the security of the network infrastructure and safeguard systems and applications from potential threats, the following measures shall be implemented: (a) Separate responsibilities or tasks of network and computer operations to mitigate unauthorized access and modification; (b) Place network equipment in a physically secure location, free from risks such as flooding, vibration, and dust; (c) Control and limit access to network equipment, permitting only authorized personnel; (d) All equipment shall adhere to the Final Acceptance Test (FAT) during installation and configuration; (e) Ensure all outgoing and incoming traffic passes through a firewall; (f) Installation of network monitoring tools and network security tools such as software sniffers or network analyzers on user computers are prohibited unless authorized by ITD Management; (g) Install an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) to detect intrusion attempts and other activities posing threats to IIUM systems and information; (h) Install a Web Content Filter on the Internet Gateway to prevent prohibited activities; (i) Any third-party network connection that physically attaches to IIUM network must receive permission from ITD Management; (j) Unauthorized network devices are prohibited from being used in the IIUM network. (k) Wireless LAN (WLAN) must implement security controls.	ICT System Administrators, IT Staff

(l) Authorization from ITD Management is mandatory for any network connection from a third party such as remote tunnelling, etc. into the IIUM network system; and (m) Ensure compliance to the Procedure for IIUM Network Services and Standard for IIUM Wireless Networking.	
0607 Media Management	
Objective: Safeguard ICT assets from exposure, modification, transfer, or destruction, and disruption of service activities.	
IIUM-060701 Delivery and Transfer	
Obtain permission from the Head of Department before sending or transferring any classified media in accordance with the Guideline on Information Classification and Labelling;	All Staff
IIUM-060702 Media Handling Procedures	
The following statements shall be adhered to: (a) Ensure proper labeling of all media based on the sensitivity level of the information. (b) Restrict and specify media access solely to authorized users. (c) Control and restrict the distribution of data or media solely for authorized purposes.	All Staff

(d) Monitor and record all media maintenance activities to prevent damage and unauthorized exposure. (e) Store all media securely in a designated and safe location. (f) Dispose of or destroy media containing classified information in accordance with established and secure procedures. (g) Ensure compliance with the Guideline on Information Classification and Labelling	
IIUM-060703 System Documentation Security	
The following shall be observed in ensuring the security of system documentation is as follows: (a) Ensure that the documentation storage system has security features; (b) Provide and enhance the security of the system documentation; and (c) Control and record all activities of access to existing systems documentation. (d) Ensure compliance with the Guideline on Information Classification and Labelling	ICT System Administrators, IT Staff
0608 Information Exchange Management	
Objective: Ensure the security of information exchange between IIUM and external agencies.	
IIUM-060801 Information Exchange	

The following must be adhered to: (a) Establish formal information or data controls within the ICT system to safeguard information transmitted through various communication facilities; (b) Media containing information should be protected from unauthorized access, misuse, or damage during transfer out of IIUM; and (c) The information contained in the electronic mail should be well protected.	All Staff, OSIC
IIUM-060802 Electronic Mail Management (E-mail)	
The followings must be adhered to: (a) Utilize only accounts or email addresses provided by IIUM; (b) The use of accounts belonging to others or sharing of accounts is strictly prohibited. (c) Ensure that every email account conforms to the format specified by IIUM. (d) Ensure that the subject and e-mail content is relevant and refers to the same subject matter being discussed before sending.	All Staff

(e) Official emails must be sent using an official email account, and the recipient's email address must be verified for accuracy. (f) Exercise caution by avoiding the opening of emails from unknown or suspicious senders. (g) Prior to transmitting transaction information via email, users must identify and verify the identity of the communicating party. (h) Delete non-essential emails that have been acted upon and no longer hold archival value. (i) Respond promptly to emails and take swift action as required. (j) Official purposes should not involve the use of private email addresses such as yahoo.com, gmail.com, streamyx.com.my, etc. (k) Users are responsible for updating and utilizing their respective mailboxes. (l) Ensure compliance with Procedure on Email Services.	
0609 Electronic Commerce Services	
Objective: Implement measures to control the sensitivity of applications and information within this service, aiming to prevent risks such as information misuse, theft, and unauthorized changes.	
IIUM-060901 Online Services	

The following must be adhered to: (a) Information used in online transactions must be safeguarded against fraudulent activities, contract disputes, and unauthorized disclosure and modification. (b) Ensure the protection of information involved in online transactions to prevent incomplete transmission, misdirection, modification, disclosure, duplication, or unauthorized repetition of messages. (c) Safeguard the integrity of information provided for systems accessible to the public or other interested parties, preventing any unauthorized modifications.	All Staff
IIUM-060902 General Information	
The following must be adhered to: (a) Ensure the software, data, and information are protected with an appropriate mechanism; (b) Ensure that the systems that are accessible to the public are tested beforehand; and (c) Ensure that all information to be displayed has been endorsed and approved before uploading to websites.	All Staff
0610 Monitoring	
Objective: Ensure detection of unauthorized information processing activities.	
IIUM-061001 Auditing and ICT Forensics	

CSIRT must be responsible for recording and analysing the following: (a) Any intrusion attempts into IIUM ICT systems; (b) Malicious code attacks, denial of service, spam, forgery phishing intrusion, threats, and physical loss; (c) Modification of hardware features, software, or any of the system components without the knowledge, direction, or consent of ITD Management; (d) Activities for surfing, keeping or distributing obscene material, defamatory and propaganda; (e) Activities involving the establishment of unauthorized services; (f) The installation and utilization of software which burdens bandwidth of the network; (g) E-mail and network abuse activities; and (h) Unauthorized IP address changing activities of other than as provided for by ICT System Administrators.	CSIRT, ICT System Administrators
IIUM-061002 Audit Trail	
Every system must have an audit trail. An audit trail records the activities that occur chronologically in the system to allow for screening and reconstruction in the event of any rearrangement or changes to the system. Audit trail shall contain the following information: (a) A record of critical transactions; (b) The audit trail information contains the user's identity, the sources used, change information, dates and times of activities, networks and applications used;	ICT System Administrators

(c) The user access activity to the ICT system is either valid or otherwise; and (d) Details of abnormal system activity or activity that does not have security features. The ICT Systems Administrator is responsible for reviewing audit trail records and, when deemed necessary, generating reports to identify any previous unusual activities. It is essential to safeguard audit trails from harm, loss, deletion, tampering, and unauthorized alterations.	
IIUM-061003 Log System	
ICT Systems Administrators shall perform the following: (a) Establish a log system to record all internet daily activities of users; (b) Periodically review the system log to detect errors that may cause disruptions to the system and take immediate action for corrective measures; and (c) In other invalid activities such as information theft and hacking, ICT System Administrators shall report these events to ICTSO and CDI/O.	ICT System Administrators, IT Staff
IIUM-061004 Log Monitoring	
The following must be adhered to:	ICT System Administrators

(a) Audit log which records all activities should be prepared and kept for an agreed period to assist in investigations and access control monitoring; (b) Procedures for monitoring use of information processing facilities should be established and the results should be monitored regularly; (c) The facilities for recording and log information should be protected from any modified and unauthorized access; (d) The administrative activities and system operations need to be recorded; (e) Fault, error and or abuse must be recorded in logs, analyzed and appropriate action taken; and (f) The time related to information system processing in IIUM, or the security domain should be consistent with an agreed point of time.	

ARTICLE 7: ACCESS CONTROL

ARTICLE 07 ACCESS CONTROL

0701 Access Control Procedure

Objective:

Control access to information.

IIUM-070101 Access Control Requirements

Access to processes and information should be controlled according to the safety requirements and job functions of different users. It needs to be recorded, updated, and support existing user access control policies. Access control regulations should be established, documented, and reviewed based on service and security requirements. The following must be adhered to: (a) Access control over ICT assets based on security requirements and user roles; (b) Access control over network services; (c) Ensure the security of information obtained via facilities (e.g. laptop) or mobile devices (d) Control over information processing facilities.	ITD, ICT System Administrators

0702 User Access Management	
Objective: Control user access to IIUM ICT assets implement control.	
IIUM-070201 User Accounts	
Users are responsible for the ICT systems they use. To identify users and their activities, the following steps should be followed: (a) Only accounts provided by the University can be used; (b) User accounts must be unique and reflect the user's identity; (c) Initially created user accounts should have the minimum access level, limited to viewing and reading only. Any changes to access levels must obtain approval from the owner of the ICT system beforehand; (d) Ownership of a user account is not an absolute right and is subject to University's rules and regulations. Accounts can be revoked if their usage violates rules and regulations; (e) Usage of another person's account or sharing accounts is prohibited; (f) Ensure compliance to the Procedure for Electronic Accounts; and (g) ICT system administrators may suspend and terminate user accounts for the following reasons: i) Job role change; ii) Retirement; or iii) Termination of service.	All Staff, ICT System Administrators

IIUM-070202 Access Rights	
The assignment and usage of access rights need to be subjected to strict control and supervision based on the requirements of the job scope.	ICT System Administrators
IIUM-070203 Password Management	
The selection, usage, and management of passwords as the primary means to access information and data in the system must adhere to best practices and procedures established by IIUM, as follows: (a) Under any circumstances and reasons, passwords must be protected and not shared with anyone; (b) Users should change their passwords when a password leak or compromise is suspected; (c) Users must ensure their passwords meet the specified length requirements outlined in the Standard for Electronic Accounts.; (d) Passwords should be memorized by the users and MUST NOT be written down, stored, or disclosed in any way; (e) Passwords for screen savers should be activated, especially on computers in shared spaces;	All Staff, ICT System Administrators

(f) Passwords should not be displayed during input, in reports, or any other media, and should not be hardcoded in programs; (g) Enforce password change during the first login or after the first login or after a password is reset/default password, except for hardware or software with limited password capabilities; (h) Passwords should be different from the user's identity; (i) Set a login attempt limit of up to 5 times for critical systems; (j) Avoid the reuse of recently used passwords; and (k) Compliance to the Standard for Electronic Accounts.	
IIUM-070204 Clear Desk and Clear Screen	
All information in any form of media must be stored systematically and securely to prevent damage, theft, or loss. Clear Desk and Clear Screen mean not leaving sensitive materials exposed either on the user's desk or on the screen display when the user is not present. Compliance measures include: (a) Using password-protected screen saver or log out when leaving the computer; (b) Sensitive materials should be stored in locked drawers or filing cabinets; and	All Staff

(c) Ensure that all documents are promptly retrieved from printers, scanners, fax machines, and photocopiers;	
0703 Network Access Control	
Objective: Preventing unauthorized usage and unauthorized access to network services in IIUM.	
IIUM-070301 Network Control	
Access control for network services must be ensured securely by: (a) Placing or installing appropriate interfaces between the IIUM network, other agency networks, and the public network; (b) Monitoring for ICT network services; and (c) Compliance with Procedure for IIUM Network Services and Standard for IIUM Wireless Networking.	ICT System Administrators, IT Staff
IIUM-070302 Internet Access	
The following must be adhered to: (a) The use of the Internet in IIUM shall be continuously monitored by the ICT System Administrator to ensure its usage is only for authorized purposes. This vigilance will help protect against the entry of malicious code, viruses, and materials that should not be in the IIUM network. (b) Content Filtering methods must be implemented to control Internet access. (c) The Internet should be used for official purposes only.	ICT System Administrators

(d) The browsed websites should only be related to the field of work. (e) Materials and data obtained from the Internet should be verified for accuracy and authenticity. As a best practice, references to Internet sources should be stated. (f) Official materials should be reviewed and approved by the Head of Departments of relevant offices before being uploaded to the Internet. (g) Users are only allowed to download legitimate materials and shall be responsible. (h) Ensure compliance with the Policy for Responsible Use of ICT Resources for IIUM Staff and Students. (i) Users are prohibited from engaging in the following activities: i. Uploading, downloading, storing, and using unlicensed software and any applications such as electronic games, videos, and songs that may impact internet access levels; and ii. Providing, uploading, downloading, and storing materials, speech texts, or content containing elements of obscenity, gambling, or violence. .	All Staff

0704 Operating System Access Control	
Objective: Prevent unauthorized access and unauthorized use of operating system.	
IIUM-070401 Operating System Access	
Control of operating system access is necessary to prevent any unauthorized access. Security features within the operating system should be utilized to block access to computer system resources. These features should include: (a) Identifying the identity, terminal, or location for each authorized user; and (b) Recording successful and failed access attempts. The methods used should be capable of supporting the following: (a) Authenticating authorized users; (b) Establishing an audit trail for all operating system access, especially for superuser-level users; and (c) Generating alerts if there is a violation of system security rules. Compliance requirements include the following: (a) Controlling access to the operating system using secure logon procedures; (b) Establishing a unique identification (ID) for each user, only to be used by that specific user; (c) Limiting and controlling program usage; and	ICT System Administrators, IT Staff

(d) Restricting the connection time to a high-risk application.	
IIUM-070402 Smart Cards	
The following compliance requirements pertain to the use of Smart Cards must be adhered to: (a) Smart Cards must be used to gain access to the designated areas. (b) Smart cards shall be kept in a safe place to prevent theft or use by any other unauthorized party; (c) Sharing of Smart Cards for access purposes is strictly prohibited, and any misuse of a Smart Card will result in its immediate deactivation. (d) Incidents involving the loss, damage, or attempts at misuse of Smart Cards must be promptly reported to the OSEM.	All Staff
0705 Application and Information Access Control	
Objective: Prevent unauthorized access and unauthorized use of information contained in system applications.	

IIUM-070501 Application and Information Access	
Aimed at protecting application systems and existing information from any form of unauthorized access that could cause damage. To ensure the strength of system and application access controls, the following should be adhered to: (a) Users should only use information systems and applications authorized according to specified access levels and information sensitivity; (b) User transactions on critical system activities should be recorded (logged) to monitor and track any unauthorized actions. (c) Implement Multi-Factor Authentication (MFA) as an additional security measure for online systems.	ICT System Administrators, IT Staff
0706 Mobile Devices and Remote Working	
Objective: Ensure information security while using mobile devices and remote working facilities.	
IIUM-070601 Mobile Devices	
The following statements shall be adhered to: (a) Record the use of mobile computing devices for loan, temporary use, or shared activity~~,~~ to detect any loss or damage; and (b) Mobile devices should be stored and locked in a secure place when not in use.	All Staff

IIUM-070602 Remote Working	
The following statements shall be adhered to: Protective measures should be taken to prevent the loss of equipment, unauthorized disclosure of information, and misuse of facilities.	All Staff

ARTICLE 8: SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

ARTICLE 08

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

0801 Security in Developing Systems and Applications

Objective:

Ensure all systems developed either internally or by third parties apply appropriate ICT security features.

IIUM-080101 Information System Security Requirements

The following statements shall be adhered to: (a) The acquisition, development, improvement, and maintenance of systems should consider security controls to ensure the absence of any errors that could disrupt processing and compromise information accuracy; (b) Security testing should be conducted on input systems to verify the validation and integrity of entered data, on processing systems to determine whether programs run correctly and without error, and on output systems to ensure the accuracy of processed data; and (c) Ensure compliance with Procedure on Management of Quality Test and UAT.	System Owners, ICT System Administrators, ICTSO

IIUM-080102 Data Input and Output Validation	
The following statements shall be adhered to: (a) Input data for applications must be validated to ensure that the entered data is accurate and appropriate; and (b) Output data from applications must be verified to ensure that the generated information is correct.	System Owners and ICT System Administrators
0802 Cryptography Control	
Objective: Protect confidentiality, integrity, and authenticity of the information through cryptographic controls.	
IIUM-080201 Encryption	
The following statements shall be adhered to: (a) Users shall always encrypt sensitive information or confidential information; and (b) Any process that involves obscuring or replacing sensitive information or confidential information shall be done by authorized individuals.	All Staff
IIUM-080202 Electronic Signatures	
The use of electronic signatures is required for relevant users based on needs.	All Staff

IIUM-080203 Public Key Infrastructure (PKI)	
Management of PKI must be carried out effectively and securely to protect the associated keys from being altered, destroyed, and disclosed throughout the validity period of those keys.	All Staff
0803 System File Security	
Objective: Ensure that system files are controlled and handled safely and securely.	
IIUM-080301 System File Controls	
The following statements shall be adhered to: (a) The system file updating process can only be carried out by ICT system administrators or relevant personnel. (b) Updated system code or configurations can only be implemented or used after testing; (c) Control access to program code or program configurations needs to be checked and monitored to prevent unauthorized modifications, deletions, and theft; (d) Test data should be carefully selected, protected, and controlled; and (e) Enable an audit log to record all updating activities for statistical, recovery, and security purposes.	System Owners, ICT System Administrators

0804 Security in Development and Support Process	
Objective: Protect and ensure the security of information systems and applications.	
IIUM-080401 Change Control Procedures	
The following statements shall be adhered to: (a) Changes or modifications to information systems and applications systems must be controlled, tested, recorded, and verified before implementation; (b) Critical applications need to be reviewed and tested when there are changes to the operating system to ensure there are no adverse effects on the University's operations and security. Specific individuals or groups should be responsible for monitoring improvements and corrections made by third parties; (c) The control changes and/or amendments made to software packages need to be monitored closely to ensure that any changes are limited to the required specifications only; (d) Access to the source code of applications should be restricted to authorized users; (e) Prevent any opportunities for information leakage; and (f) Ensure compliance with Procedure on Management of Quality Test and UAT and Procedure on Management of IT Change.	System Owners, ICT System Administrators

IIUM-080402 Outsourced Software Development	
Outsourced software development shall be supervised and monitored by the system owner. The source code for all applications and software is the property of the Government of Malaysia.	ITD
0805 Control of Technical System Vulnerabilities	
Objective: Ensure control of technical systems vulnerabilities is effective, systematic, and consistent by responding appropriately to ensure effectiveness.	
IIUM-080501 Control of Technical Threats	
Control of technical vulnerabilities should be implemented on the operating system and application systems in use. The following statements shall be adhered to: (a) Obtaining accurate technical vulnerability information in a timely manner for the information systems in use; (b) Assessing the exposure level to identify the potential risks to be faced; (c) Ensure that control measures are implemented to address the associated risks; and (d) Ensure that any codes that is written in the application system and operating system will not have any potential risk to the organization's information security.	ICT System Administrators

ARTICLE 9: ICT SECURITY INCIDENT MANAGEMENT

ARTICLE 09

ICT SECURITY INCIDENT MANAGEMENT

0901 ICT Security Incident Reporting Mechanisms

Objective:

Ensure that incidents are promptly and effectively managed to minimize the impact of ICT security incidents.

IIUM-090101 Reporting Mechanism

Security incidents in ICT refer to adverse events that occur on ICT assets or threats that may lead to such occurrences. It could involve actions that violate ICT security policies, whether explicitly or implicitly stated. ICT security incidents such as the following should be reported to the IIUM CSIRT team promptly: (a) Loss or unauthorized disclosure of information, or suspected loss or disclosure to unauthorized parties; (b) Unauthorized use of information systems or suspected unauthorized usage; (c) Loss, theft, or disclosure of passwords or access control mechanisms, or suspected loss, theft, or disclosure; (d) Unusual system events such as file loss and frequent system failures; (e) Attempts of intrusion, misconduct, and unexpected incidents; Processes involved in reporting of ICT security incidents at IIUM must comply to the Procedure of Management of IT Service Request and Incident.	All Staff

0902 ICT Security Incident Information Management	
Objective: Ensure a consistent and effective approach is used in the management of information security incidents in ICT.	
IIUM-090201 ICT Security Incident Information Management Procedures	
Information regarding managed ICT security incidents should be stored and analysed for planning purposes, reinforcement actions, and learning to control the frequency, damage, and costs of future incident occurrences. This information is also used to identify incidents that occur frequently or have a high impact on IIUM. Evidence materials related to ICT security incidents should be stored and organized. Controls to be considered in the collection of information and incident management are as follows: (a) Keeping audit trails, regularly backing up, and protecting the integrity of all evidence materials; (b) Keep copies of evidence and records of all copying activity information; (c) Establishing contingency plans and activating service continuity plans; (d) Providing immediate recovery actions; (e) Notifying or seeking advice from legal authorities if necessary; and (f) Ensure compliance with the Procedure of Management of IT Services Request and Incident.	ICTSO, CSIRT

ARTICLE 10: DISASTER RECOVERY MANAGEMENT

ARTICLE 10

DISASTER RECOVERY MANAGEMENT

1001 Disaster Recovery

Objective:

Ensure that service operations are uninterrupted and continuous service delivery to customers is maintained

IIUM-100101 Disaster Recovery Plan (DRP)

DRP is a critical component of any organization's strategy to ensure service continuity, even in the face of unexpected disruptions or disasters. Developing a comprehensive DRP is essential to taking a holistic approach to maintaining service continuity. This is to ensure that there is no disruption in the processes in the delivery of the organization services, the following points should be noted: (a) The University needs to identify the severity of events that can disrupt the business processes; (b) The University needs to identify all responsibilities and emergency or recovery procedures; (c) The University needs to implement emergency procedures to allow recovery to be done as soon as possible or within the specified time frame; (d) The University needs to document and record all processes and procedures that is essential to ensure that everyone in the	ITD Director, DRP Coordinator

University or team understands how to perform their responsibilities effectively; (e) The University needs to conduct training programs on emergency procedures; (f) The University needs to create backups to ensure the safety and recovery of data in various contexts; and (g) The University needs to do testing and update the plan (if necessary) at least once a year. A DRP should be developed and should include the following: a) List of core activities that are considered critical in order of priority. b) List of IIUM personnel and vendors with contact details. c) List of information that require backups and the location it is stored together with the information recovery instructions and related facilities. d) Alternative processing resources and location to replace the resources that have been paralyzed. Storing a copy of DRP in a separate location to protect it from damage during a disaster is a crucial aspect of DRP planning. Additionally, regular testing, evaluation, and updates of the plan are essential to ensure its effectiveness and relevance. Scheduling tests and exercises for the DRP is essential to ensure that all members involved understand the plan, their responsibilities, and their roles during its implementation. IIUM should ensure that copies of the Disaster Recovery Plan (DRP) are constantly updated and protected as effectively as the main Disaster Recovery Plan (DRP) document.	

ARTICLE 11:

COMPLIANCE

ARTICLE 11 COMPLIANCE	
1101 Compliance and Legal Requirements	
Objective: Increase the level of ICT security to prevent breach and violations of the IIUM ICT Security Procedure.	
IIUM-110101 Procedure Compliance	
Every user in IIUM must adhere to and comply with the ICT Security Procedure, IT Policies and Guidelines, and IT Regulations that are enforced. All IIUM ICT assets, including information stored in IIUM property belong to the University. Heads of Department/authorized officers reserve the right to monitor users' activities to detect illegal usage. Any use of IIUM ICT assets other than the meaning and intended purpose, further elaborated in Procedure for Responsible Use of ICT Resources, will be considered a misuse of IIUM resources.	All Staff
IIUM-110102 Compliance with Policies, Standards and Technical Requirements	
ICTSO shall ensure that all ICT security procedures within their scope of work comply with the ICT policies and guidelines, standards and technical requirements. Information systems should be checked regularly to comply with the ICT security standards.	ICTSO ICT System Administrators

IIUM-110103 Compliance with Personal Data Protection	
All users have a duty to ensure that any personal data processing activities comply with the principles outlined in the Personal Data Protection Act 2010 (PDPA). This includes: (a) Obtaining consent for the collection and processing of personal data; (b) Processing personal data only for lawful purposes directly related to the University's activities; (c) Ensuring data collected is not excessive and is relevant to the purpose of processing; (d) Keeping the data subject informed about their personal data processing though a clear Procedure; (e) Ensuring personal data is not disclosed beyond the original purpose of processing or to people not originally intended without consent; (f) Safeguarding personal data against loss, misuse, unauthorized or accidental access or disclosure, alteration, or destruction. (g) Retaining personal data only for the period necessary to fulfil the purpose of collection; and (h) Maintaining accuracy and completeness of personal data and keeping it updated from time to time by allowing data subjects to access and correct their personal information. Users must familiarize themselves with these principles and apply them in their daily operations and usage of the ICT facilities in the University. Should there be reasonable suspicion of personal data breach occurs it should be reported immediately to the University.	~~All User~~ All Users

IIUM-110104 Audit Requirements Compliance	
Compliance to audit requirements is necessary to minimize threats and maximize effectiveness of the information systems audit process. Audit requirements and inspection activities of any operational system must be planned and agreed to reduce the probability of services provision disruption. Access to the information systems' audit tools should be maintained and monitored to ensure that it is not misused.	All Staff
IIUM-110105 Legal Requirements	
The following are the Acts, Order, Direction and Guidelines that must be observed by all users at IIUM: (a) Communications and Multimedia Act 1998; (b) Computer Crimes Act 1997; (c) Copyright Act 1987; (d) Cyber Security Act 2024 (Act 869); (e) Digital Signature Act 1997; (f) Electronic Commerce Act 2006; (g) Electronic Government Activities Act 2007; (h) Official Secrets Act 1972; (i) Personal Data Protection Act 2010; (j) Penal Code; (k) Online Safety Act 2025 (Act 866); (l) IIUM Anti-Bribery and Anti-Corruption Policy Notwithstanding the above, other laws may from time to time apply depending on the subject matter of the IIUM ICT Security Procedure.	All Staff All Student

IIUM-110106 Best Practices	
The following are the references that will be adapted as the best practice which must be observed by all users at IIUM: (a) Director General Letter of Instruction - Stabilization Measures for Implementation of Electronic Mail System in Government Agencies, dated 23 November 2007; (b) General Circular No. 1 of 2001 entitled "Security Incident Reporting Mechanism Information and Communication Technology (ICT); (c) General Circular No. 2 Year 2000 - The Role of Committees under IT Committee and Government Internet Committee (GITIC); (d) General Circular Number 3- year 2009 - Guidelines for the Public Sector Network and ICT System Security Level Evaluation, dated 17 November 2009, (e) General Circular No. 3 of 2000 entitled "Government Information Technology Security Policy and Communications"; (f) General Circular No. 4 Year 2006 - Public Sector Information and Communication Technology (ICT) Security Incident Handling Management; (g) General Circular Number 6 Year 2005 - Security Risk Assessment Guidelines for Public Sector; (h) General Orders; (i) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002; (j) MAMPU Director General Letter of Instruction - Measures Concerning the Use of Electronic Mail on Government Agencies, dated June 1, 2007;	

(k) MAMPU Director General Letter of Instruction - Business Continuity Management for Public Sector Agencies, dated January 22, 2010. (l) MAMPU ICT Standard Operating Procedure (SOP); (m) National Secretary General Letter of Instruction - Steps to Strengthen Security Wireless Local Area Network in Government Agencies, dated October 20, 2006; (n) Public Administration Development Circular No. 1 year 2003 entitled "Guidelines on the Procedure of Internet and Electronic Mail Usage in Government Agencies"; (o) Treasury Circular Letter (First Supplementary) No. 2/1995 – Procedure for Preparation, Assessment, and (p) Treasury Circular Letter. No.3/1995 - Consultancy Services Acquisition Regulation; (q) The Direction of the Treasury; (r) Security Directive; Notwithstanding the above, other policies, directives, circular, orders, guidelines and procedures may from time to time apply depending on the subject matter of the IIUM ICT Security Procedure.	
IIUM-110107 Procedure Violation	
Violation of IIUM ICT Security Procedure may lead to disciplinary action.	All Staff

Glossary

Term	Definition
Appointed service provider (third parties)	Company or person chosen to perform specific tasks or services for another organization based on an agreement or contract.
Applications	Software program that runs on a web server and is accessed by users through a web browser. Unlike desktop applications, which are installed on a local computer, web applications function on the internet using web technologies such as HTML, CSS, JavaScript, and server-side programming languages (e.g., PHP, Python, Java)
CD/IO	Chief Digital/Information Officer
Critical Equipment	Equipment that are in data centre and Internet Gateway Centre (IGC).
Critical Systems	Systems that are rated severe and high under risk assessment
CSIRT	Computer Security Incident Response Team
DRP	Disaster Recovery Plan
DRP Coordinator	A person responsible for planning, implementing, coordinating, and maintaining the University's disaster recovery plan and strategies in alignment with ISO standard requirements. The DRP Coordinator ensures that critical information systems and services can be restored and made operational within defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) following a disruption, disaster, or major incident.
Electronic Signature Media	The various formats or platforms used to create, transmit, and verify electronic signatures.
Electronic Signature	An encrypted electronic stamp of authentication that confirms the integrity, authenticity, and non-repudiation of a message or document.

Head of Department	Head of Kulliyyah, Center, Division, Institute, Office, Mahallah (KCDIOM)
ICT	Information and Communication Technology.
ICT Assets	All information and communication technology resources such as hardware and software that are available to the organization and require protection to ensure their confidentiality, integrity and availability.
ICT Hardware	Physical devices and equipment that is involved in processing, storing and sharing data and information.
ICT Resources	ICT Resources means ICT facilities including the IIUM network, appliances, servers, computers, computing laboratories. All associated networks in classrooms, lecture theatres and video conferencing rooms across the University. Internet access both wired and wireless, email, hardware, data storage, computer accounts, software (both proprietary and those developed by the University), communication (telephone) services and voicemail.
ICT System Administrator	A person responsible for managing and maintaining computer applications, computer systems, network devices and information infrastructures.
ICT Security Team	Team that manages ~~IT~~ Cyber Security in the University.
ICTSO	Information and Communication Technology Security Officer is a person responsible for protecting an organization's ICT systems from cyber threats by assessing risks, implementing security measures, monitoring for breaches, and ensuring compliance with security standards.
IIUM	The International Islamic University Malaysia, otherwise known as the “University”.
ICT ~~IT~~ User	A person who uses computers or IT devices.
ITD	Information Technology Division.

ITD Management	CD/IO, Director, Senior Deputy Directors, Deputy Directors and Team Leaders.
ISMS	Information Security Management System
ISMS Steering Committee	A group of key stakeholders and decision-makers within the University tasked with overseeing the development, implementation, maintenance, and continuous improvement of the University's Information Security Management System
ISMS Task Force Committee	A specialized group within the University dedicated to the hands-on implementation, monitoring, and maintenance of the Information Security Management System
ISMS Working Committee	A group of personnel within the University responsible for actively implementing and maintaining the organization's information security procedures. They carry out day-to-day responsibilities relating to security policies, processes, and practices to guarantee that the organization's information is safeguarded from various risks.
Document Controller	A person responsible for endorsing, managing, controlling, and maintaining all Information Security Management System documents and records in compliance with the standard's requirements. The role ensures that all policies, procedures, guidelines, and records are properly developed, reviewed, approved, updated, distributed, stored, and securely disposed of in a systematic and controlled manner.
KCDIOM	Kulliyyahs/Centres/Divisions/Institutes/Offices/Mahallah in IIUM
LAN	A collection of devices connected in one physical location
Media	Refers to method and tools used to share information around the organization.
Mobile Code	Software or code that is transmitted across a network and runs on a remote device without the user's direct installation. It is used in web-based applications and includes technologies like JavaScript

	or ActiveX. Mobile code can pose security risks, such as spreading malware or bypassing security controls.
Mobile Devices	Laptops/notebooks/tablets procured using the University's budget (excluding computer allowances).
NACSA	National Cyber Security Agency, Malaysia
Network-connected	All devices that are connected by wire, optical cables, or wireless to the digital telecommunication networks that are owned and/or operated by the University.
OSIC	Office for Strategy and Institutional Change
OSEM	Office of Security and Management.
SASMEC	Sultan Ahmad Shah Medical Centre
Shared Mobile Devices	Mobile devices that are shared and used by multiple users within the University.
Staff	Any person employed under a contract of service with the University (as defined in Constitution of IIUM)
Student	Any undergraduate student, postgraduate student, part-time student, student under distance learning or off-campus programme, diploma student, matriculation student, exchange and nongraduating student of the University (as defined in Constitution of IIUM)
System Files	Critical files necessary for the proper operation of an operating system or software application which include configurations, libraries, drivers, and executables that the system relies on to manage hardware, control processes, and run applications.
System Owner	A person or team responsible for managing and overseeing a specific system or application and ensure the system runs well, follows policies, and meets business needs.
Third parties	Any external individual, organization or entity that is not part of the University that interacts with its information system and data.

User	Individuals who utilize the University's ICT resources and have access to its systems, networks, and data for academic, administrative, and operational activities.
User Credential	A username and password authentication token that is bound to a particular user.
University ID	Unique identifier assigned to students, staff, and faculty members within a university system. It is often used for various administrative and academic purpose.
UTICTEC	University Technical ICT Sub-Committee

Appendix 1

COMPLIANCE DECLARATION
IIUM ICT SECURITY PROCEDURE

Name (Capital Letters) : …….

Identity Card Number : …….

Position : …….

Department : …….

It is solemnly and sincerely declared that: -

1. I have read, understood, and agreed to comply with the provisions contained in the IIUM ICT Security Procedure, which is available on the IIUM website or can be obtained through the ITD Director's office via the following channels:
   - Email : ltd-dir@iium.edu.my
   - Phone : 03-6421 4876

2. If I breach any of the provisions described in the IIUM ICT Security Procedure, appropriate action can be taken against me.

Signature: .....

Date: .....

Appendix 2

LIST OF PROTECTED AREAS IN IIUM

No.	Location	Campus
1	IIUM Data centre (SASMEC)	Kuantan
2	IIUM Data Centre (Gombak)	Gombak
3	IIUM Data Centre (Kuantan)	Kuantan
4	Internet Gateway Centre	Gombak