INTERNATIONAL ISLAMIC UNIVERSITY

MALAYSIA

ICT SECURITY POLICY

IIUM POLICY DOCUMENT

PREPARED FOR:
International Islamic University Malaysia

PREPARED BY:
Information Technology Division

Document Change Log

Release Version	Date	Pages Affected	Remarks/Change Reference
Version 1.0			

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Shahidah Mahbob	Policy Reviewed and Vetted by OLA	09/04/2019	09/04/2019
Shahidah Mahbob	Submission to ICT Committee No 2/2019	12/12/2019	16/12/2019

1. OBJECTIVE

1.1 This ICT Security Policy shall apply to all ICT Resources, IT Users and IT Administrators with the aim to prevent, detect and respond to unauthorized access, usage and modification of information, system and network, with the aim to ensure business continuity.

1.2 The goal of this policy is to preserve:

a) Confidentiality of information by protecting classified electronic information from unauthorized disclosure or intelligible interception.

b) Integrity of information and ICT infrastructure by safeguarding the accuracy and completeness of information, software and ICT infrastructure.

c) Availability of information, services and ICT infrastructure by ensuring that Information and vital services are available to users when required.

1.3 This policy is to create a level of awareness among IIUM IT Users and IT Administrators regarding the need for security in day-to-day operations and their respective roles and responsibilities.

2. TERMS AND DEFINITIONS

Term	Definition
IIUM	The International Islamic University Malaysia, otherwise known as the "University".
ICT	Information and Communication Technology.
ITD	Information Technology Division.
ITD Management	CIO, Director, Deputy Directors and Team Leaders.
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.
ICT Resources	ICT Resources means ICT facilities including the IIUM network, 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), telephone services and voicemail.
ICT Security Team	Team that manage ICT Security in the university.
IT User	A person who uses computers or IT devices.
IT Administrator	A person responsible to manage and maintain computer application, computer systems, network devices and information infrastructures.
Critical systems	Systems that are rated severe and high under risk assessment
User credential	A user name and password authentication token that is bound to a particular user.
Permanent Staff	Permanent staff appointed to fill vacant positions and retire at the compulsory retirement age. Only Malaysians are eligible to be appointed as permanent staff.
Contract Staff	Contract staff appointed to fill in vacant positions and serve for a minimum 12 months with the University. Staff on contract does not enjoy certain benefits applicable to permanent staff.

3. RESPONSIBILITIES OF IT USER

3.1 General Security

3.1.1 The IT User is responsible for ensuring security, integrity, backup and recovery of university data and information on IT equipment and electronic storage devices in their custody.

3.1.2 The IT User is responsible for the security and confidentiality of the data and information which they obtain access to.

3.1.3 All IT Users are accountable for all use of IIUM systems performed using their user credential.

3.1.4 All IT Users are to immediately inform the IIUM Security Team on becoming aware of any loss, compromise, or possible compromise of information, or any other incident which has ICT security implications.

3.2 Network Security

3.2.1 The network security for ICT Resources shall be in compliance with the IIUM Policy for Network Services.

3.2.2 ICT Resources which require public, non-VPN access from the internet shall be located in a designated data centre facility operated by the ITD/Centre of Studies and Administration Offices.

3.2.3 All outgoing connections are subject to network monitoring and filtering.

3.2.4 Actions prohibited are as follows:

a) Any attempt to access restricted information and to evade traffic analysis is strictly prohibited. Exemptions are applied to appointed auditors and security administrators.

b) Activities which interfere with network operations including P2P connection, mega upload file sharing and transparent onion routing are strictly prohibited.

c) Attaching any new or additional network devices, including but not limited to servers, printers, hubs, PCs, to the IIUM network without prior approval from ITD is prohibited.

d) Changing security-related devices and network settings on supplied IT equipment including but not limited to PC network cards without prior approval from ITD is prohibited.

e) Physical access to IT equipment such as network equipment rack, wireless access points are strictly prohibited. Exemptions apply to authorized technical personnel.

f) Setting up of critical Internet services, including but not limited to routers, gateways, mail, web, news servers, other than part of teaching and learning course module, without authorization from ITD, are strictly prohibited.

g) Inbound network connections other than via the authorized gateways such as setting up dial-up servers, are strictly prohibited.

h) Simultaneous network connection, e.g. simultaneous LAN and broadband connection are strictly prohibited.

3.3 System Security

3.3.1 All users of system and application with passwords are to comply with the Policy for Electronic Accounts.

3.3.2 Workstations, computers terminals, notebook computers and PCs, must not be left unattended in a state whereby unauthorized parties could gain access to the system and data. It is recommended to use password protected screen saver and auto log-out or auto session termination, upon a specified idle limit.

3.3.3 Physical access to critical servers, such as entering the Data Centre, without prior authorization from ITD is strictly prohibited.

3.3.4 Dealing, distributing, installing, or using unlicensed or pirated software is strictly prohibited.

4. RESPONSIBILITIES OF IT ADMINISTRATOR

4.1 General Security

4.1.1 Maintenance and security of computer labs should be managed by the respective

Academic and Administrative Offices.

4.1.2 IT Administrators are to comply with this policy for all systems under their control.

4.1.3 IT Administrators are to conduct their own backup of data and system.

4.2 Network Security

4.2.1 Systems that are to provide access from the internet will be located in the data centre operated by the ITD/ Centre of Studies and Administration Offices.

4.2.2 Systems that are to provide access to only the private LAN are to be located in a dedicated server room and connected to the network *via* separate LAN from the user LAN.

4.2.3 The management of security devices shall be in compliance with the procedure for management of security devices.

4.3 System Security

4.3.1 The management of systems shall be in compliance with the IIUM Procedure for Management of Computing Systems and Servers.

4.3.2 Privilege and administrative access on a system and its data should be restricted to authorized users.

4.3.3 Critical systems shall be equipped with preventive and detective security controls, with audit trail of a minimum of 6 months storage.

4.3.4 IT Administrators are responsible for ensuring access is revoked for suspended and resigned personnel. Any common passwords known by suspended or resigned staff, must be changed on the date of their departure.

4.3.5 IT Administrators are responsible for ensuring the system and application is free from known vulnerabilities that can lead to compromise of the goal of this policy. Measures including patch management and AV signature updates.

4.3.6 Disaster recovery and contingency procedures for critical systems, shall be in place, and tested periodically.

4.3.7 Written procedures shall exist to ensure proper system maintenance and operational management by authorized and trained personnel.

4.3.8 Operational system changes are to be implemented in a non-disruptive manner such as performing tests and vulnerability assessments prior to live production.

4.3.9 Contracts with external parties, who deal, use, develop or maintain the system shall include provision stating that they are bound by this policy and failure to comply shall be treated as breach of contract.

4.3.10 Administrators are to ensure programs and data owned by a resigned personnel to be transferred to another authorized party before their departure becomes effective, in order to avoid irrecoverable data loss.

4.4 Server Security

4.4.1 The management of servers shall be in compliance with the IIUM Policy for Management of Computing Systems and Servers.

4.4.2 Ownership and responsibilities:

4.4.2.1 An operational group under ITD and respective Centre of Studies and Administrative Offices shall own servers deployed at respective data centre and server rooms.

4.4.2.2 Servers shall be registered to the enterprise management system and be kept up-to-date. The following information shall be recorded to identify (at minimum):

a) server contact(s), location and backup contact;

b) hardware and operating system/version; and

c) main functions and applications.

4.4.3 General Configuration Guidelines shall be referred as follows:

4.4.3.1 Operating system configuration shall be in accordance with accepted best practice.

4.4.3.2 Services and applications that will not be used shall be disabled, where practical to do so.

4.4.3.3 Access to services shall be logged and/or protected through access control methods.

4.3.3.4 The most recent application patches shall be installed.

4.3.3.5 Console access *via* privilege accounts such as root and administrator access is not allowed unless necessary. Usage of non-privileged account is recommended.

4.3.3.6 Remote administrator access shall be *via* secure and encrypted connection e.g. *ssh* and *sftp*.

4.3.3.7 Servers are to be located in a secure area, with physical access control.

4.5 Monitoring

4.5.1 All security related events on critical system shall be logged. The security log shall be retained for a minimum of 6 months.

4.5.2 Any security related events shall be reported to ITD Service Desk or the IT Security Team and action to be taken in compliance with the IIUM Policy for IT Service Desk and Incident Management. Logs shall be reviewed and severe incidents are reported to Top Management. Corrective measures shall be prescribed. Security incidents include but not limited to:

a) Port scan;

b) Evidence of unauthorized access; and

c) Anomalous activities on the network.

4.5.3 System and network monitoring shall be conducted to ensure compliance and measure effectiveness of security controls. Non-compliance activities shall be reported to the IT Security Team for further action.

5. ITD ROLES AND RESPONSIBILITIES

5.1 All users and IT Administrator's roles and responsibilities shall also apply to ITD.

5.2 ITD shall liaise and consult with the relevant office in charge of safety and security, or external parties, to ensure adequate site security, fire prevention procedures, health and safety primarily for the data centre. The data centre shall be managed according to the IIUM Policy for the Management of IIUM Data Centre.

5.3 ITD shall maintain on-going security awareness among IT Users and IT Administrators, including regular awareness program, training and online publications.

5.4 ITD shall ensure access rights to network, system and application are restricted on need-to-know basis.

6. HUMAN RESOURCES (HR) ROLES AND RESPONSIBILITIES

6.1 All IIUM personnel are required to sign a contract of employment that establishes their roles with respect to both physical and information security.

6.2 Staff transfers, suspensions, terminations and resignations shall be immediately notified to ITD so that access can be immediately revoked.

7. PENALTIES AND NON-COMPLIANCE

The Director of ITD is responsible to take necessary actions in the event of violation of this policy.

8. MAINTENANCE OF POLICY

ITD is responsible for the formulation and maintenance of this policy.

9. RELATED POLICIES

This policy shall be read together with the IIUM:

a. ICT Regulations
b. Electronic Data Management Policy
c. Policy for Electronic Accounts
d. Policy for IIUM Network Services
e. Policy for responsible use of ICT Resources (IIUM Staff)
f. Policy for responsible use of ICT Resources (IIUM Student)
g. Management of IT Service Request and Incident
h. Management of IIUM Data Centre

i. Disaster Recovery Plan