Guideline for Responsible Use of ICT Resources -DRAFT

IIUM ICT GUIDELINES

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	23-JUL-2012	Whole document	New policy
Version 2.0	July 2024	Whole document	Revision of policy to guidelines
Version 2.0	October 2025	4,5,15	ABMS and ISMS Clause, Reference Document

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Assoc. Prof. Dr. Abd Rahman Ahlan, ITD	Submission to ICT Committee Meeting No. 02/2012	23/07/2012	31/07/2012
Siti Zarina binti Muhamat	Submission to ITD Management Meeting No.14/2024	18/09/2024	24/09/2024
Syed Hazrul Syed Salim	Submission to ITD Management	28/10/2025	

1. OBJECTIVE

The objective of this guideline is to ensure the responsible, ethical, and legal use of ICT resources by IIUM staff and students. This policy aims to protect the integrity, security, and reliability of ICT resources, promote respect for intellectual property and privacy rights, and prevent misuse that could harm individuals or the University.

2. SCOPE

2.1 This guideline applies to all staff and students of IIUM, including full-time, part-time, and contract employees, as well as all students enrolled in any capacity;

2.2 The ICT resources provided are to support teaching and learning, research, consultancy and administrative activities of the University.

3. TERMS AND DEFINITIONS

Term	Definition
IIUM	The International Islamic University Malaysia, otherwise known as the “University”
ICT	Information and Communication Technology
ICT Resources	All ICT facilities including computers, computing laboratories, all associated networks in classrooms, lecture theatres, mahallahs 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; owned, leased or provided by the University.
ITD	Information Technology Division

4. GUIDELINE STATEMENTS

4.1 General Use

4.1.1 This guideline shall be implemented in accordance with IIUM’s Anti-Bribery Management System (ABMS) in compliance with **ISO 37001:2025** requirements to ensure transparency, integrity, and accountability in all processes. All processes, decisions, and activities under this guideline must uphold the principles of integrity, transparency, and accountability, and shall be free from any form of bribery or corruption.

4.1.2 This guideline shall be implemented in accordance with IIUM's ICT Security Procedure in compliance with **ISO/IEC 27001:2022** requirements to ensure confidentiality, availability and integrity in all processes. All processes, decisions, and activities under this policy/guideline must uphold the principles of confidentiality, availability and integrity as to protect the information data and assets.

4.1.3 Respect for Law and University Policies

4.1.3.1 IIUM is committed to provide a secure, respectful, and productive environment through the effective management and use of its ICT resources;

4.1.3.2 Users must comply with all relevant laws, regulations, and University policies when using ICT resources;

4.1.1.2 Unauthorized access, use, alteration, or destruction of any ICT resources is prohibited;

4.1.1.3 The University shall not defend or support any user who uses ICT resources for unlawful purposes.

4.1.4 Respect for Others

4.1.4.1 Users must respect the rights and privacy of others, refraining from activities that may cause harm, offense, or distress to others;

4.1.4.2 Harassment, bullying, and discrimination through any ICT resources are strictly prohibited;

4.1.4.3 ICT resources must not under any circumstances be used to humiliate, intimidate, offend, or vilify others on the basis of their race or gender.

4.1.5 Academic Integrity

Users must uphold the principles of academic integrity, ensuring that all work submitted is their own and appropriately acknowledging all sources of information.

4.2 Access Control

4.2.1 Granting of Access and Entitlement

4.2.1.1 Access to ICT Resources must be approved by the relevant authority. Access must be given based on a need to access that ICT resource and is subject to the availability of those resources;

4.2.1.2 Access to ICT resources may be granted by ITD, while access to Kulliyyah-owned resources or facilities is granted by the respective Kulliyyah. The Administrator of the ICT facilities may restrict access to any user found in breach of this policy;

4.2.1.3 User are granted access to the University resources, sensitive data, and to external networks on the basis that their use of ICT resources shall be responsible, ethical, and lawful at all times.

4.2.1.4 Users may access the internet for educational, research and work- related purposes. Personal use is also allowed, provided it is lawful and reasonable in terms of time and cost to the University.

4.2.1.5 All staff and matriculated students of IIUM are entitled to have access to the University's network. External party of the University shall be given the network access via wireless connection with restricted usage time.

4.2.2 Access Upon Contract Expiry or Authorized Access Period

4.2.2.1 Email, computer and system access will cease on expiration of contract or end of services;

4.2.2.2 For strictly professional or work-related reasons, staff and other authorized users may request that email access to be extended for a period of up to 30 days; upon approval by ITD Management.

4.2.3 Restrictions to Access

4.2.3.1 Users are prohibited from accessing accounts, data or files on IIUM ICT resources without authorization;

4.2.3.2 The Administrator of the ICT resource may restrict access to user on the grounds that the user is in breach of this policy.

4.2.4 Third Party Access

Entities other than the ITD may neither negotiate nor grant third party access to the University's applications, databases, communications and network infrastructure.

4.3.1 Access to and Monitoring of Equipment

4.3.1.1 The University reserves the right to access and monitor any computer or electronic device connected to the IIUM network, whether owned by the University or personal equipment such as laptops connected to the network;

4.3.1.2 Access to and monitoring of equipment is permitted for any reason; including, but not limited to, suspected breaches by the user of his/her duties as IIUM staff or students, unlawful activities or breaches of University legislation and policies;

4.3.1.3 Access to and monitoring of equipment includes, but is not limited to email, web sites, server logs and electronic files. The University may keep a record of any monitoring or investigations.

4.3 Security and Privacy

4.3.1 Data Protection

4.3.1.1 Users must handle personal and sensitive data with the utmost care, adhering to the University's policies and guidelines;

4.3.1.2 Data and information relating to persons and other confidential matters acquired for business purposes shall be protected;

4.3.1.3 Unauthorized access, sharing, or distribution of personal or confidential information such as credentials, password or PINs, is prohibited;

4.3.1.4 The University business information shall be protected from unauthorized and/or accidental disclosure;

4.3.1.5 Users may be required to sign a Non-Disclosure Agreement prior to authorization being granted for access to certain ICT Resources.

4.3.1.6 User accounts, files and stored data, including email messages at the University are kept private and secured from access by others, including ITD staff;

4.3.1.7 Users should be aware that ITD staff may from time to time become aware of the contents of user directories and hard disk drives during the normal course of their work, and are obligated to keep the information confidential;

4.3.1.8 Users should understand that authorized ITD staff may need to intervene in user accounts, temporarily suspend account access, or disconnect computers from the network to maintain the University's ICT resources, including repairing, upgrading, or restoring file servers or personal computer systems.

4.3.2 Device and Network Security

4.3.2.1 Users must ensure that all devices connected to the university's network are secured with up-to-date antivirus software and other necessary security measures;

4.3.2.2 Unauthorized installation or use of software that compromises the University network security is prohibited;

4.3.2.3 Users are prohibited from using the IIUM network to gain unauthorized access to any computer account or system, attempt to bypass data protection measures, exploit security vulnerabilities, or mask the identity of a computer account or machine;

4.3.2.4 Users are prohibited from deliberately interfering with the normal operations of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with any component of a local area network (LAN), Intranet, or wide area network (WAN), blocking communication lines; or interfering with the operational readiness of a computer;

4.3.2.5 Users are prohibited to installing, run, or give to another user a program that is intended to or is likely to damage a file or computer system and/or reproduce itself on the University computer systems, including but is not limited to, programs known as Trojan horses, viruses, root kits, or worms.

4.3.3 Domain Name Registration

4.3.3.1 All domain names for IIUM projects/ activities must be registered through ITD;

4.3.3.2 Ownership and control of the site belong exclusively to the University, not to the individual who registers the name.

4.3.4 Software License Restrictions

Use of licensed software is subject to terms of license agreements between the IIUM and the software owner or licensor, and may be restricted in its use.

4.4 Responsible Usage

4.4.1 Appropriate Use

4.4.1.1 ICT resources must only be used for academic, administrative, and research purposes;

4.4.1.2 Users must ensure all ICT resources allocated to them are used responsibly and in accordance with the University's policies and guideline;

4.4.1.3 Users must not compromise the security of any ICT resources, nor exploit or attempt to exploit any security deficiency;

4.4.1.4 The account authorized to the user are not transferable. Sharing of passwords or allowing others to use one's account is strictly prohibited;

4.4.1.4 Users must use strong passwords and change them regularly to protect their accounts;

4.4.1.5 Users must take reasonable steps to ensure physical protection, including safeguarding against damage from improper use, food and drink spillage, managing electrical power effectively, implementing anti-static measures, preventing theft and etc.;

4.4.1.6 User must ensure computers are not left unattended without first logging out and securing area, especially when connected to computer system containing sensitive and valuable information.

4.4.2 Resource Management

4.4.2.1 Users should refrain from excessive use of bandwidth and storage space, and should not engage in actions that waste computing resources or unfairly monopolize them. Examples including but not limited to, sending junk mail, chain letters, playing games, initiating unnecessary jobs or processes, obtaining unnecessary output, generating excessive network traffic, or printing an excessive number of copies;

4.4.2.2 Activities that degrade the performance of ICT resources or impede others' use are prohibited.

4.4.3 Confidential Information

All users are responsible for maintaining the confidentiality of:

i. All University data, unless the information has been approved for external publication;
ii. Information provided in confidence to the University by other entities;
iii. Users are obligated not to disclose University business information unless authorized to do so.

4.4.4 Personal Use of ICT Resources

Users are permitted to use ICT resources for limited personal purposes, provided that it is lawful, does not negatively impact the user's work performance, hinder the work of other users, or harm the University's reputation, image, or operations. Such use must not result in noticeable additional costs to the University.

4.4.5 Private Commercial Use of ICT Resources

ICT Resources must not be used for personal profit or private commercial purposes.

4.5 Personal Web Pages

4.5.1 Publication of Personal Web Pages

4.5.1.1 Staff is permitted to publish personal web pages on computers connected to the IIUM network. The contents on these pages must comply with all applicable laws of the country;

4.5.1.2 The University reserves the right to regularly monitor personal web page / sites hosted on IIUM servers, and may remove, or request the user to remove or alter, any content that does not comply with these standards;

4.5.1.3 Special care must be taken to ensure that the web pages/ sites do not infringe on any third-party copyrights, including audio or video files, music charts/ lyrics, photographs, text or etc.

4.5.2 Disclaimer Required on Personal Web Pages

Every personal web page hosted on IIUM's servers must prominently display the IIUM Personal Page Disclaimer on each page. This disclaimer clarifies that the website is not endorsed by IIUM and that any views or opinions expressed on the pages are solely those of the author and not representative of the University.

4.5.3 Responsibility for Personal Web Pages

User is responsible for legal issues related to their personal web pages. The University will not defend the user in legal actions arising from content on their personal site, nor will it be liable for any damages awarded against the user by a court or commission.

4.6 Email and Messaging

4.6.1 Users Responsibility for Using Email and Messaging

When using the email or messaging system, users must at all times:

i. Respect other's privacy and personal rights;
ii. Avoid copyright infringement;
iii. Avoid plagiarism and defamation;
iv. Not forward or copy emails containing personal information without permission;
v. Not send forged messages or use someone else's e-mail address or password without authorization;
vi. Not send mass distribution or advertising emails without authorization;
vii. Ensure recipients consent to emails, do not send SPAM;
viii. Not harass, intimidate or threaten others;
ix. Not send sexually explicit materials;
x. Maintain civility in all communications;
xi. Refrain from sending angry or antagonistic messages that may be perceived as bullying or threatening;
xii. Refrain from personal commercial use of email and messaging systems.

4.6.2 User Email Spam Management

User must adhere to the following:

i. Do not respond to emails requesting confidential information, such as usernames, passwords, or bank account details;
ii. Treat all emails from unknown senders as spam and move them to the Junk Mail folder;
iii. Use a separate email address for public forums, newsgroups, and mailing lists, and avoid using IIUM email address to prevent spam;
iv. Use multiple email addresses for different purposes to identify different sources and allow for more effective email filtering;
v. Remove IIUM email address from personal websites and use web-based forms to significantly reduce spam;
vi. Avoid purchasing from companies that send spam; refrain from visiting their websites or requesting further information, as most of their offers are scams;
vii. Utilize email filters to manage emails effectively;
viii. Report spam to ITD to help compile useful statistics for setting spam policy;
ix. Report any fraudulent or illegal content in unsolicited emails to ITD.

4.5 Intellectual Property

4.5.1 Users must abide the intellectual property rights, ensuring proper licensing for software and acknowledging sources of information, complying with software licensing agreements and contracts related to the University's ICT resources;

4.5.2 Unauthorized reproduction or distribution, or use of copyrighted material without authorized permission is prohibited.

4.6 Software-based Video Conferencing

4.6.1 Users are permitted to use software-based video conferencing tools such as Zoom, Google Meet, and Microsoft Teams for educational, research, and work-related purposes;

4.6.2 Personal use of software-based video conferencing tools is allowed, provided it is lawful, does not interfere with work performance, does not hinder others, and does not incur noticeable additional costs to the University;

4.6.3 Users must adhere to the following guidelines when using software-based video conferencing tools:

i. Respect the privacy and personal rights of others during video conferences;

ii. Avoid sharing or distributing confidential University information without proper authorization;

iii. Ensure that any recordings of video conferences are conducted with the consent of all participants;

iv. Use appropriate and professional language and behaviour during video conferences;

v. Follow all relevant University policies, including those related to data protection and intellectual property rights.

4.6.4 The University reserves the right to monitor the use of software-based video conferencing tools to ensure compliance with these guidelines and other University policies.

4.7 Prohibited Use of ICT Resources

4.7.1 Advertising and Sponsorship

Paid advertisements are prohibited on any website using IIUM domain name, or any site closely associated with the University, unless authorized in writing by the University authority.

4.7.2 Peer-to-Peer File Sharing (P2P)

The use or installation of peer-to-peer file sharing software on the University's network is prohibited. Exceptions for legitimate teaching or research use must be approved by the University authority.

4.7.3 Pornography

Users are prohibited from using the University's ICT Resources to access, create, store or distribute any type of pornographic material.

4.7.4 Gambling

Users are prohibited from using the University's ICT resources for gambling activities.

4.7.5 Computer Games

Game playing using IIUM ICT resources is strictly prohibited, except when it forms a formal component of a University academic subject or is part of a Kulliyyah, Centre, or Division-sponsored event.

4.7.6 Assignment Services

IIUM students are prohibited to use ICT resources to sell or purchase assignments, or to offer to write assignments or to request help with assignments.

4.7.7 No Business Activities

Users are prohibited from conducting business activities or publishing journals or magazine using IIUM ICT resources unless authorized by the University.

4.7.8 Student Computing Laboratories

Users are required to abide by all the rules and guidelines set by the relevant authorities.

4.7.9 Databases, Online Journals, eBooks

The use of electronic resources provided by IIUM is governed by individual license agreements and is restricted to non-commercial research and study purposes. Users must adhere to the use restrictions specified on the respective sites or in the license agreements. It is prohibited to systematically download, distribute, or retain substantial portions of information without authorization.

4.8 University's Liability

The University accepts no responsibility for:

i. Loss or damage, including consequential loss or damage, arising from personal use of the University's ICT resources; or

ii. Loss of data or interference with personal files arising from the University's efforts to maintain the ICT resources.

5. IMPLEMENTATION AND NON-COMPLIANCE

The Director of Information Technology Division holds the responsibility for the implementation of this guideline and shall take necessary actions in the event of violation of this policy.

6. ENFORCEMENT

This guideline is applicable to all IIUM staff and students and any infringement of the policy may subject to disciplinary actions.

7. MAINTENANCE OF GUIDELINE

The Information Technology Division is responsible for the formulation and maintenance of this guideline.

8. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

This guideline shall be read together with the following or any documents which recently approved:

8.1 IIUM ICT Policy
8.2 ICT regulations
8.3 IIUM Information Management Policy
8.4 IIUM ICT security procedure
8.5 IT Infrastructure Library(ITIL)
8.6 Control of Business IT(COBIT)
8.7 Any other related IIUM ICT policies