INTERNATIONAL ISLAMIC UNIVERSITY

MALAYSIA

Policy for Email Services

IIUM ICT 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	23-JUL-2012		

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Azhar Mahmood, ITD	Initial draft	11/11/2008	_
Azhar Mahmood, ITD	Reviewed by ICT Policy Review Committee Meeting No. 2/2008	19/11/2008	_
Azhar Mahmood, ITD	Approved by ICT Council No. 1/2009	_	30/01/2009
Azhar Mahmood, ITD	Reviewed by ICT Regulation Meeting No. 2/2010	15/4/2011	

1. OBJECTIVE

1.1 The objective of this document is to define the policy for IIUM email services provided by the University.

1.3 This policy covers all email services including account entitlement, security and misuse of email account.

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
Email account	An email account is the location where mail is actually delivered. It is a combination of a login username and password and disk space
DMLA	Delegated Mailing List Administration
IT Coordinator	Academic staff appointed by the Rector to oversee ICT matters at the centre of studies

3. POLICY STATEMENTS

3.1 Email Entitlement

3.1.1 Email account is provided for use to the University's academic staff, administrative staff and student.

3.1.2 Email account is provided to all full-time staff, contract staff, Academic Trainee, undergraduate and postgraduate students.

3.1.3 Part-time staff is not entitled to an email account.

3.1.4 IIUM subsidiaries staff is not eligible to have the University email account.

3.2. Email as Official Records

3.2.1 Email is a corporate asset of the University. Access to email is granted to facilitate the teaching and learning, research, academic, administrative and business activities of the University. The content of the email messages remain the property of the University.

3.3 Email Security

3.3.1 A user is responsible for maintaining the security of his email account and password.

3.3.2 A user shall change his password regularly and log out when the computer or terminal is unattended.

3.3.3 Email messages sent using the University email service shall not be encrypted in any way and shall not be used for confidential communications.

3.3.4 Users are advised to scan attachments for viruses and not to open any attachment from unknown senders.

3.4 Email Management

3.4.1 Email client that are supported by ITD are as follows:

3.4.1.1 Microsoft Outlook

3.4.1.1 Google Gmail

3.4.1.2 Other email client software may be used but without support from ITD.

3.4.2 Individual email users are responsible for managing their own email account.

3.4.3 Email storage is as provided by Google which is currently 30GB per user, this may change as per Google policy.

3.5 Email Backups

3.5.1 Google and Microsoft guarantees 99.9% up-time and availability.

3.6 Change of Email Address

3.6.1 A unique email address shall be used as an identity to access various systems in the University such as portals and other application systems and shall be used during the staff tenure with the University. Therefore, an email address is not allowed to be changed unless with valid reasons. Any application to change an email address shall be officially submitted and subject to approval by ITD.

3.7 Deletion of Email Account and Messages

3.7.1 Deletion of email messages shall be managed by the user, keeping in mind storage levels and archival levels.

3.7.2 User shall be responsible to manage their university email.

3.7.3 If a staff is terminated or leaves the University, the email account and the messages stored in the University servers shall be deleted in accordance with the policy.

3.8 Email Distribution List and Groups

3.8.1 Creation of an official mailing list should be made to ITD; stating the purpose, the name of the mailing list and the manager of the mailing list who will be responsible for deletions and additions of members.

3.8.2 User are allow to create mailing list or collaborative inbox. Whereas, the creator will be the owner and administrator of the group.

3.8.3 Mailing lists shall be used for the purpose of teaching and learning, research, administrative matters and University related student activities.

3.8.4 The list should be for official use and internal consumption only.

3.8.5 The official list should not include any external email addresses.

3.8.6 Creation of a mailing list should consist of 5 members or more.

3.8.7 The list should not be publicized to external parties e.g. include in CCs.

3.8.8 Only members are allowed to send an email to the distribution list. Non-members that need to send email to the list should request permission from ITD.

3.8.9 Any changes to the DMLA should be communicated to ITD by the IT Coordinator.

3.8.10 Users may create their own mailing list in which may contain external email addresses and they will be responsible for the mailing that they created.

3.9 Google Apps

3.9.1 Usage of Google Apps will be terminated once staff members leave the company

3.9.2 File which is stored inside Google Drive will be deleted regardless of its value after staff members leave the company.

3.9.3 Google Apps usage will solely depend on the user, ITD will not be responsible for action taken by the user.

3.10 Misuse of Email

Prohibited activities include, but are not limited to:

3.10.1 Sending or soliciting obscene, profane or offensive material.

3.10.2 Sending email messages that contain discriminating or sexually harassing material or messages that creates an intimidating or hostile work or study environment for others.

3.10.3 Using University email facilities in the conduct of personal businesses.

3.10.4 Unauthorized forwarding of University restricted messages.

3.10.5 Using copyrighted information in a way that infringes the copyright.

3.10.6 Unauthorized use of another person's mailbox.

3.10.7 Chain letters, junk mail or other forms of useless mass mailing are not allowed.

3.10.8 Any deliberate actions to compromise, damage or disrupt the system such as worms, viruses and similar are strictly prohibited.

3.10.9 Activities that cause congestion and disruption of networks and the system.

3.10.10 Applying for a user account under false pretenses.

3.10.11 Fraudulent, harassing and obscene messages or materials are not allowed in all forms: transmitting, forwarding, printing and storing.

3.11 The University reserves the right to:

3.11.1 Access individual staff University email for security and legal purposes.

3.11.2 Terminate any email account or privilege which content is unethical.

3.11.3 Terminate the execution of any process that consumes excessive system resources with or without prior notification.

3.11.4 Terminate the email service of staff that has resigned or is no longer working in IIUM. Staff must do migration of email before the date of end of service. However, a user can request to extend the access to the mailbox for a period not exceeding 30 days.

3.12 **Accessing email in mobile phone**

3.12.1 ITD will provide support and assistance for mobile using Android OS.

3.12.2 Other mobile which using other than Android OS will not be support by ITD. However user are free to use it at will.

4. IMPLEMENTATION AND NON-COMPLIANCE

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

4.2 This policy is applicable to all staff and student of the University and any infringement of the policy may subject to disciplinary actions.

5. ENTITIES AFFECTED BY THIS POLICY

5.1 Staff members and students who are eligible for email services are affected by this policy.

6. MAINTENANCE OF POLICY

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

7. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

7.1 ICT Regulations 2012

7.2 ICT Security Policy

7.3 (IIUM/ITD/ICTPOL/6.2) Guideline for Email Announcement

7.4 (IIUM/ITD/ICTPOL/6.3) Guideline for Email Spam