Badr University in Cairo

(BUC)

Use of Email Policy

Approvals

Approval	Name	Date	Signature
BUC President	Prof.Dr. Mostafa Kamal	10/01/2019	
General Secretary	Dr. Mohamed Soliman	10/01/2019	
Edited By			
Quality Assurance Manager	Pro.Dr. Abdellatif Ahmed	20/12/2018	
IT Manager	Eng. Said Saleh	01/01/2019	
Revision Date		**01/01/2021**	

Table of Contents

Purpose for the policy :

The purpose of this policy is to describe the acceptable use of the University's email and related services, systems, and facilities.

The Policy is maintained and regulated by Computer Services and is cross-referenced to, and by, a number of other University policies and regulations.

The Policy will be made available to users of the email and related services and facilities. There will also be periodic review of the Policy and, if necessary, amendment from time to time. This will be necessary with regard to the expected development of the system, the operational use of the system and generally recognized best practice.

Email services are provided by the University to support its primary role of education and research and associated functions related to this role. See Who can have an account for details of categories of people who are eligible for access to computing facilities.

Policy Statement:

This policy is intended to detail the rules of conduct for all members (generally staff and students) of the **Badr University** who use email and related services.

This Email Policy applies to the use, for the purpose of sending or receiving email messages and attachments, of any IT facilities, including hardware, software, and networks, provided by the University. The Policy is applicable to all members of the University including staff, students and other authorized users of University IT facilities.

Only authorized users of the University computer systems are entitled to use email facilities. All members of the University who agree and abide by the University regulations, are entitled to use computing facilities and email systems at all times when the network is available.

Who needs to know this policy?

The Policy is maintained and regulated by Computer Services and is cross-referenced to, and by, a number of other University policies and regulations.

The Policy will be made available to users of the email and related services and facilities. There will also be periodic review of the Policy and, if necessary, amendment from time to time. This will be necessary with regard to the expected development of the system, the operational use of the system and generally recognized best practice.

Email services are provided by the University to support its primary role of education and research and associated functions related to this role. See Who can have an account for details of categories of people who are eligible for access to computing facilities.

Scope of this Policy

This Policy applies to all members of the University community who need to activate and actively maintain an BUC Email account and to all members of the community who connect computer systems to the campus network, BUC-NET.

Policy Specifications

1- Acceptable use

1.1 General

The University's main purpose in providing IT facilities for email is to support the teaching, learning, research, and approved business activities of the University. IT facilities provided by the University for email should not be abused. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):

- creation or transmission of material which brings the University into disrepute.
- creation or transmission of material that is illegal.
- the transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind
- the unauthorized transmission to a third party of confidential material concerning the activities of the University.
- the transmission of material such that this infringes the copyright of another person, including intellectual property rights.

- activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users.
- activities that corrupt or destroy other users' data or disrupt the work of other users.
- creation or transmission of any offensive, obscene or indecent images, data or other material.
- creation or transmission of material which is designed or likely to cause annoyance, inconvenience or anxiety.
- creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs
- activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals.
- creation or transmission of anonymous messages or deliberately forging messages or email header information, without clear identification of the sender).
- the unauthorized provision of access to University services and facilities by third parties.

1.2 Personal use

The University permits the use of its IT facilities for email by students, staff and other authorized users for a reasonable level of personal use. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):

- a level of use that is not detrimental to the main purpose for which the facilities are provided.
- priority must be given to use of resources for the main purpose for which they are provided.
- not being of a commercial or profit-making nature, or for any other form of personal financial gain.
- not be of a nature that competes with the University in business.
- not related to any use or application that conflicts with an employee's obligations to the University as their employer.
- not be against the University's rules, regulations, policies and procedures and in particular this email policy.

1.3 Research and related

It is recognized that, in the course of their work or research, individuals of the University may have a requirement to transmit or receive material that would normally be defined as offensive, obscene, indecent or similar. In the case of properly supervised or lawful research purposes it is acceptable to do so. If in doubt advice should be sought.

2- Quotas and limits

All users have access to the centrally managed email server. All accounts have quota limits placed on them. All file partitions are backed up to tape on a regular basis. Accounts that are removed will have their files archived in accordance with the Account Closure and User Accounts policies. Unless specifically requested no archiving takes place.

Users receive email notification when approaching their quota limit and are encouraged to follow guidance in this email to manage their account. The final email that is received which takes an individual over their limit will always be delivered. Once over quota no further email can be delivered to an individual's inbox until they have reduced their storage below their limit. Email that fails to be delivered because a user is over quota is held in the local mail queues for four days and the system will retry periodically to deliver. After four days the email is returned to sender.

3- Best Practices in Use of Email

Malware
BUC email users should be careful not to open unexpected attachments from unknown or even known senders, nor follow web links within an email message unless the user is certain that the link is legitimate. Following a link in an email message executes code, that can also install malicious programs on the workstation.

Identity Theft
Forms sent via email from an unknown sender should never be filled out by following a link. Theft of one's identity can result.

Password Protection
BUC's policy requires the use of strong passwords for the protection of email. A strong password must contain digits or punctuation characters as well as letters. In addition, your email password should be different from your BUC network password.

Departmental Email Boxes
Departments that provide services in response to email requests should create a shared mailbox to help support departmental functional continuity for managing requests sent via email.

Forwarding Email
BUC email users may choose to have their email delivered to a CIS-managed or contracted mailbox or forwarded to another mail repository. However, a non-BUC forwarding address should not be used if there is a reasonable expectation that confidential information will be

exchanged. Email is not considered a secure mechanism and should not be used to send information that is not considered public.

Staff email users on an extended absence should create an Out Of Office message, which should include the contact information for another staff member who can respond while the user is away from the office.

Staying Current

Official University communications such as urgent bulk email, course email should be read on a regular basis since those communications may affect day-to-day activities and responsibilities.

Compromised Accounts

An email account that has been compromised, whether through password-cracking, social engineering or any other means, must be promptly remedied with the appropriate means. The appropriate means will include a password reset, review of account settings, computer scans and malware disinfection to prevent possible leakage, spamming, potentially infecting others and degradations of network service.

If the account is being used to harm others at BUC and the owner cannot be reached in a reasonable period of time ("reasonable" being driven by the negative impact to the BUC community), the Director of Information Technology Security will direct the office of Computing Accounts and Passwords (CAP) to reset the password. Should the same account be compromised three or more times in any 12-month period, the account will be immediately suspended, and will not be re-enabled until the user notifies the Director of Information Technology Security to ensure that all remediation has taken place, and is provided with remedial training.

Lists

Email lists can be created. Generally individuals requesting a list will be responsible for the ownership and management of the list.

4- Logging

Traffic through the Computer Services email gateways is logged. Logs include details of the flow of email but not the email content. Transaction logs are kept online for up to a month. Backups of these logs are kept for up to 3 months. Logs are available to authorized systems personnel for diagnostic and accounting reasons.

5- Spam and junk mail

Spam can be defined as "the mass electronic distribution of unsolicited email to individual email accounts". Junk mail is usually a result of spamming. Spam and junk mail are regarded as interlinked problems.

Incoming email is checked against other Realtime Blackhole Lists and if successfully matched is marked locally with the insertion of an additional header flag. Email matching the databases is NOT blocked, it is simply marked and passed as normal. There are methods individuals can use to filter this email.

6- Remote access

Remote access to Badr University email servers (for reading email) is possible via the Internet.

Remote access to other POP3 or IMAP mailboxes off campus is permitted via secure methods only.

7- Incident handling and data protection

The University will investigate complaints received from both internal and external sources, about any unacceptable use of email that involves IT facilities. IT in conjunction with other departments as appropriate, will be responsible for the collation of information from a technical perspective. It should be noted that logs are only kept for limited periods of time so the prompt reporting of any incidents which require investigation is recommended.

Where there is evidence of an offence it will be investigated in accordance with the University's disciplinary procedures applicable to all members of the University. In such cases IT will act immediately with the priority of preventing any possible continuation of the incident. That is, accounts may be closed or email may be blocked to prevent further damage or similar occurring.

Revision History

Version	Date	Modified Areas
0.1	January, 2019	_
0.2	January 2021	