DEPARTMENT OF INFORMATION TECHNOLOGY
BRAC UNIVERSITY IT POLICIES

INDEX

DEPARTMENT OF INFORMATION TECHNOLOGY

1. IT POLICIES AND GUIDELINES

BRAC University has several policies in place to protect the University as well as the faculty, staff and students of the Institution. BRAC University wants to now put into place this document where policies for using its computer and network are well defined so that misuse of IT related equipment are prevented.

All users of BRAC University computer network agree to abide by the following policies and guidelines as applicable, in terms of Acceptable use policy, Password policy and email use and retention policies.

2. Department of Information Technology Acceptable Use Policy

2.1 Overview

As part of its educational mission, BRAC University acquires, develops, and maintains computers, computer systems and networks. These computing resources are intended for University-related purposes, including direct and indirect support of the University's instruction, research and service missions; University administrative functions; student and campus life activities; and the free exchange of ideas within the University community and among the University community and the wider local, national, and international communities. Appropriate use of computers and information networks includes adherence to the normal requirements of ethical and legal behavior in an academic community.

2.2 Purpose

This policy is designed to outline the various responsibilities that users have to have with regard to their use of network resources in order to protect the University, its faculty, staff and students from electronic and legal harm resulting from improper use of information technology.

2.3 Scope

This policy applies to all users of BRAC University computing resources, whether affiliated with the University or not, and to all users of those resources, whether on campus or from remote locations.

Additional policies may govern specific computers, computer systems or networks provided or operated by specific units of the Academic Institution.

2.4 Policies

Users who connect to BRAC University's network must abide by the acceptable use policy described here, as well as any relevant campus computing policy and all relevant laws of the Peoples Republic of Bangladesh, regulations, and contractual obligations. The use of BRAC University's technology resources is a privilege, which may be revoked if users fail to comply with these policies.

2.5 Rights and Responsibilities

The rights of academic freedom and freedom of expression apply to the use of BRAC University computing resources. So too, however, are associated, the responsibilities and limitations associated with those rights. The University supports a campus and computing environment open to the free expression of ideas, including unpopular points of view. However, the use of BRAC University computing resources, like the use of other university-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system or network does not extend to whatever is technically possible. It is strictly prohibited to use BRAC University's IT resources to hurt the religious sentiments of any religious, social and cultural groups.

2.6 User Responsibilities

As an user of Information Technology resources of the University, you have the following responsibilities:

- You are responsible for registering your network devices with BRAC University's Network Access Control system in order to maintain access to the network
- You are responsible for all traffic originating from the network devices that you register regardless of whether you generate the traffic or not
- You are responsible for abiding by all applicable laws set forth by the State and Local governments
- You are responsible for protecting your privacy
- You are responsible for not violating the privacy of others
- You are responsible for keeping your network devices up to date with current security patches
- You are responsible for using anti-virus software and ensuring that such software is not more than 10 days out of date (Contact IT Department to update any anti-virus due to expire shortly)
- Once a server version anti-virus is in place, all connected PCs, laptops and any other communication device will be scanned by the installed antivirus software in the server, automatically before the boot-up process starts. You are responsible that this is done.
- You are responsible for protecting any and all sensitive data to which you have access.
- You are responsible for following all applicable BRAC University IT policies relating to your use of Information Technology resources

2.7 Security and Privacy

BRAC University employs various measures to protect the security of its computing resources and its user's accounts. Users should be aware, however, that the University cannot guarantee security and

confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly.

Users should also be aware that their uses of BRAC University computing resources are not completely private. While the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. Therefore, users of the Institution's computing resources have no reasonable expectation of privacy in what they do over the University's computer systems. The University may also specifically monitor the accounts of individual users of University computing resources, including internet browsing including individual login sessions and the content of individual communications, without notice, when:

- The user has voluntarily made them accessible to the public, as by posting to social media, web pages or other public forums;
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of the University or other computing resources or to protect the Institution from liability;
- There is reasonable cause to believe that the user has violated or is violating this policy, any other BRAC University policy, or the law;
- An account appears to be engaged in unusual or unusually excessive activity; or it is otherwise required or permitted by law.
- As part of the University's investigation or for other business purposes.

BRAC University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate disciplinary proceedings.

2.8 Commercial Use

Computing resources are not to be used for personal commercial purposes or for personal financial or other gain. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of University IT equipment.

2.9 Network Infrastructure/Routing

Users must not attempt to implement their own network infrastructure. This includes, but is not limited to, installing basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not install or create alternate methods of access to BRAC University IT resources, such as modems and virtual private networks (VPNs). Users must not offer network infrastructure services such as DHCP and DNS. Exceptions to this policy must be coordinated with the Information Technology Department of the University.

2.10 Harassment

All users must adhere to the policies set forward in the Student, Faculty, Administrator and Staff Handbooks, if any, regarding sexual and other forms of harassment. These policies apply in any

format or forum including electronic. It is punishable offence if someone uses the system to sexually harass any staff, faculty members, employees or students.

2.11 Security Breaches

Attempts to alter system software, to bypass security protocols, to introduce viruses, worms, malwares, Trojans or other malicious or destructive programs, or otherwise "to hack" are expressly forbidden. Users should never try to circumvent login procedures on any computer system or otherwise attempt to gain access where they are not authorized. Any member of BRAC University community, including a student, who intentionally breaches or willfully attempts to breach security, will be subject to disciplinary action, including suspension and dismissal.

2.12 Copyright Compliance

It is a violation of University policy and state law to participate in copyright infringement. The Institution complies with all legal requests for information and will not hesitate to provide information about users who are engaging in copyright infringement in response to a lawful request. Copyrighted materials include, but are not limited to computer software, audio and video recordings, photographs, electronic books, and written material. If you share movies or music that you did not create, you may be infringing on another's copyright. Consequences of copyright infringement can include disciplinary actions by the University authorities. In addition, copyright owners or their representatives may sue persons who infringe on another's copyright in the courts of Bangladesh.

2.13 Enforcement

Users who violate this policy may be denied access to the University's computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the University disciplinary procedures applicable to the user. The University may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, functionality and operability of the University or other computing resources or to protect the University from liability. The institution may also refer suspected violations of applicable law to appropriate law enforcement agencies.

3. Department of Information Technology
Password Policy

3.1 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of BRAC University's entire network. As such, all employees of BRAC University (including contractors and vendors with access to BRAC University systems) and students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. All use of BRAC University accounts is assumed to be performed by the person assigned to that account. Account owners are held responsible and liable for all activities with their accounts.

3.2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, frequency of change, and resetting of passwords on BRAC University systems.

3.3 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any BRAC University campus, has access to the BRAC University network, or stores any non-public BRAC University information.

3.4 Policies

In order to enhance and maintain security of the BRAC University I.T. System the following recommendations are made:

- All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed on or at least every **90 days.**
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every **180 days.** The recommended change interval is every 90 days.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.
- Initial passwords are to be set to a unique value per user. Initial password shall only be valid until the first successful user authentication and must be changed by the user after first use.
- Initial, pre-designated passwords are valid only until the first successful user authentication into an account. The user must choose their own passwords based upon the following standards and guidelines.
- All passwords are to be at least **eight (8)** characters in length.
    - Group and shared passwords are explicitly prohibited at BRAC University
    - Password complexity will be set to enforce the use of at least both alphabetic and numeric characters.
        - Must contain at least 3 letters
        - Must contain at least 2 numbers
        - Maximum number of letter pairs is 2
        - At least one special character must be in the password (@,*, # etc.)
    - Password parameters will be set to require that new passwords cannot be the same as the four(4) previously used passwords.
    - Passwords must **NOT** contain your username in any form
    - Accounts will be locked out after five failed login attempts and will remain locked for up to **90** minutes

NOTE: A strong password is important to keep away potential hackers and intruders, so users are strongly advised to use a password which cannot be easily compromised.

3.5 Password Reset

System and session idle timeout feature will be set on all systems to time out after being idle for 15 minutes. If you have forgotten your password, you should utilize the “forget password” option for

getting a new password. If this feature is not in place, you may contact the IT department to reset your password. You will be required to login via security questions that you chose and answered. If you have forgotten the answers to your security questions, you will need to present your University ID to the Information Technology Help Desk, and they will further assist you in resetting your questions and password. If you are unable to physically visit the Information Technology Help Desk, we will mail your account information to the address that we have listed in our official records. There are no exceptions to this policy.

3.6 General Password Construction Guidelines

BRAC University has multiple user ID and Password Sign-On (SO) technology to enable students and employees to use multiple username and password combination to access multiple systems and applications, such as Zimbra, Google Apps etc. BRAC University IT policies place greater importance on selecting a strong password that is difficult to guess. Students and employees are strictly prohibited from sharing their BRAC University password with anyone for any reason.

If in case University authorities introduce of SSO (Single Sign-on), then all members using the network will be capable of using one user ID and Password to access multiple systems and applications.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z) as well as numbers
- Are at least eight (8) alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Do not contain words found in a dictionary or other commonly used slang words in any form including backwards
- Do not contain trivial letter or number patterns such as aaqqqccc, qwerty, 12345678, 1233421, etc.
- Are not based on personal information such as birth dates, addresses, phone numbers, or names of family members, pets, friends, or co-workers
- Passwords should be hard to guess but easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- Have at least one special character in the password like @,#,*, ^ etc.

NOTE: Do not use any of these examples as passwords!

3.7 Password Protection Standards

Do not use the same password for BRAC University accounts as for other access (e.g., personal bank account, option trading, benefits, etc.). Do not share BRAC University passwords with ANYONE, including family members, co-workers, administrative assistants or supervisors. Passwords must never be sent in an email or instant message. Do not use the "Remember Password" feature of applications (e.g., Firefox, Chrome, Instant Messenger etc.). Passwords must never be written down or stored in a file on any computing device (including laptops, smart phones, tablets or similar

devices) without using encryption. All passwords are to be treated as sensitive, confidential BRAC University information.

BRAC University IT Department will NEVER ask you to reveal your password at any time. If you are asked to reveal your password via telephone, email, or in person by anyone claiming to be a BRAC University official or IT Department staff member, do not respond. Report the incident immediately to the IT Help Desk at: support@bracu.ac.bd and/or info@bracu.ac.bd

If an account or password is suspected to have been compromised, report the incident to the IT Help Desk and change all passwords.

3.8 Enforcement

Users who violate this policy may be denied access to BRAC University computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the BRAC University policy for disciplinary procedures applicable to the user. The University may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the institution or other computing resources or to protect the University from liability. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

4. Department of Information Technology

BRAC University e-mail Policy

4.1 Introduction:

BRAC University provides its faculty and staff with various electronic communication tools, including an e-mail messaging system, using the open source ZIMBRA. By Law all inter-departmental emails must be through the BRAC University e-mail server. The following guidelines, which govern faculty and staff use of the institution's e-mail system, apply to e-mail use at the University campus, as well as from remote locations, including, but not limited to, employee homes. The University's e-mail rules and policies apply equally to full-time employees, part-time employees, faculty members, interns, work studies, and consultants. Anyone who violates any of these e-mail rules and policies will be subject to disciplinary action, which may result in termination also.

4.2 No Reasonable Expectation of Privacy:

All e-mail communications created and transmitted using the **University e-mail system**, are the sole property of the University. Keep in mind that any message you send or receive becomes a permanent record even if you delete the message from your account. Accordingly, you should have no reasonable expectation of privacy when it comes to business and personal use of the University e-mail system.

4.3 Use of E-mail for University related Business:

Your official BRAC University e-mail account shall be considered an official means for communicating of University related business, and may in some cases be the sole means of communication. In order to stay current with University related communications, all faculty and staff personnel are expected

to read, and shall be presumed to have received and read, all official BRAC University e-mail messages sent to their official BRAC University e-mail accounts. All faculty and staff personnel are advised against using third party email services (e.g., Yahoo, Hotmail, Gmail or AOL) when conducting university business related communications. Communications with students should always be sent to their University student email address (ending in @bracu.ac.bd) from a BRAC University faculty/staff email address. This helps guarantee delivery and ensure the privacy of the communication.

4.4 Safety Considerations:

Users are to take precautions to prevent the unauthorized use of e-mail account passwords. Passwords are not to be shared with others and their confidentiality is to be strictly maintained. When choosing passwords, users should select passwords that are difficult to guess and should change them on a regular basis. Users will be held accountable for all actions performed with their accounts, including those performed by other individuals as a result of user negligence in protecting passwords.

You may, on occasion, receive malicious email claiming that “your account has expired”, “you have exceeded your mailbox quote” and so forth which either ask you to reply with your login account and password, or to click on a link which will prompt you for similar information. You should NEVER respond to such emails/click on links as legitimate as they may seem. You should also always remain vigilant of such attempts to collect your BRAC University or personal credentials. Only websites which have “bracu.ac.bd” in the address bar of your internet browser are legitimate and are safe to enter your BRAC University username and password.

Other e-mails may contain viruses as attachments therefore e-mails from unknown senders or with unexpected attachments should not be opened/double-clicked.

Emails address will be created by the IT Department for an user after an IT release form has been duly filled up and approved by competent authorities – Heads of Departments , HR, Registrar etc.

Please note that at BRAC University e-mail administrators and other computer support staff will never ask you for your password.

4.5 E-mail Monitoring Activities:

The University does not monitor the content of electronic mail as a routine procedure, but it reserves the right to monitor, inspect, copy, review, and store any and all employee e-mail use at any time and without the employee's consent. It will do so only when it believes these actions are appropriate to: prevent or correct improper use of the BRAC University e-mail system; ensure compliance with University policies, procedures, or regulations; or satisfy a legal obligation.

4.6 SPAM Policy:

The IT department has implemented an anti-spam appliance (Spam Filter) and has configured it to a reasonable degree of filtering to prevent unsolicited emails from reaching our campus community. However, the appliance may:

a) occasionally permit such emails from reaching your account and/or

b) block legitimate emails based on certain keywords, etc. In the event that you receive an unsolicited email message, please do not open it/click any links/open any attachments.

Promptly report such messages to the IT department and wait for further instruction. If you were expecting an email from a trusted source and they informed you that it was sent, you may contact the IT department to see if it may have been blocked by our anti-spam appliance at which point the e-mail will be released for delivery to you – except if it was blocked because it contained a virus.

4.7 Departmental E-mail Accounts:

In some situations, a single point of contact is required where multiple individuals could manage service requests. These accounts are permitted if the department head determines that a group account is required to conduct the business of the department and he/she will be responsible for all of the account activities, including use of it by authorized and unauthorized employees.
A policy for visiting Faculty and Teaching Assistants (TA) should be drawn out later – we would like to restrict or avoid allocating email address of BRAC University email services.

4.8 Mass E-mail & Unsolicited E-mail:

While faculty and staff can maintain their own personal mailing lists, those lists should not be used to send unsolicited e-mail that violates any of the University's policies. Commercial use of mailing lists, except for authorized University related business is prohibited. Any message to the University community at large must be first approved by an appropriate University officer (Dean, Registrar, Pro Vice Chancellor, Vice Chancellor). Maximum size of email for all BRAC University users will be restricted to 1024Kbytes when circulated by : bracu-all@bracu.ac.bd

4.9 E-mail Backups:

In the event of an e-mail system disaster, email will be restored to the state of user email accounts on that server at the time of the last backup. As e-mail messages may be received and subsequently deleted or lost since the last backup, the University cannot guarantee that all e-mail messages can be restored. Every effort is made to ensure that the e-mail system is backed up on a nightly basis.

4.10 Redirection/Forwarding of E-mail:

Redirection/forwarding of official University e-mail communications to third party email services is not permitted. This is to ensure the integrity and privacy of messages and to ensure that replies to group emails are not sent from a 3rd party email account.

4.11 E-mail Quota Size:

E-mail storage is costly and finite. As such, BRAC University e-mail accounts have a standard storage size limit of 2,048 Megabytes (MB).

One single email content size will be restricted to 15MB for in-house email and 4MB for external emails, as restrictions are also imposed by the ISPs in this regard.

4.12 E-mail Message Size Restrictions:

The largest e-mail message size that users can send or receive from anyone is 15 megabytes (MB). This includes the message text, headers, and any attachment combined. Please note that you may not be able to send large attachments to contacts that use other email services with smaller attachment limits.

The Maximum number of email circulated from a Department will be restricted to 100 emails per session.

Eligibility for circulating mail through : bracu-all should be restricted and size of this type of bulk mail transmitted through bracu-all@bracu.ac.bd should be restricted to a maximum of 1024KB.

4.13 E-mail retention policy:

All e-mail communications are retained on the University e-mail server for a period of **90 days.** Other e-mail communications older than 90 days are archived off to other storage locations for a period of three years from the origination date. After that period, unless expressly requested for, the emails will be deleted.
It is suggested that emails sent using bracu-all@bracu.ac.bd should be deleted every 3 months.

4.14 E-mail Disclaimer:

All outgoing e-mail messages will be appended with the following disclaimer: *'This email may contain confidential material. If you were not an intended recipient, please notify the sender and delete all copies. Eco-Tip: Think green before you print*'.

4.15 Employee Terminations:

Once the effective termination date has been determined by the Human Resources department, the e-mail account of a terminated employee is disabled and the mailbox contents are archived for a period of 120 days and then deleted.

4.16 Best practices when e-mailing:

When creating your e-mail messages please follow these guidelines:

1. Always include a Subject Line. A subject line describes the reason for the email, without it, the recipient is lost.
2. Start your e-mails with a salutation.
3. Do not include social security numbers, credit card numbers, or anything else of a sensitive nature in the body of or as attachments in e-mail communications (remember, an e-mail is like a postcard).
4. Do not put anything in an e-mail that you do not want forwarded.
5. Use the forwarding and carbon copy features judiciously.
6. Do not forward internal e-mails outside of the University unless there is an appropriate business reason to do so.
7. Only hit “Reply All” if you really need to reply to all.
8. End your e-mails with a signature and contact information.

4.17 Offensive Content and Harassing or Discriminatory Activities Are Banned:

Faculty and staff are prohibited from using the University e-mail system to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in

any way objectionable or offensive. Anyone receiving messages with this type of content should report the matter to their supervisor immediately.

4.18 Faculty and Staff are prohibited from using the University e-mail system to:

1. Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, color, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.
2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
3. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
4. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, disrespectful, or adult-oriented language.
5. Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, negatively impact employee productivity, or harm employee morale.

4.19 Reporting E-mail Abuse:

E-mail abuse may be reported to: aminul@bracu.ac.bd. Reports of abuse will be investigated and handled as appropriate. In all cases, do not delete any evidence or e-mail messages as they can be used as evidence.

4.20 Change Order Request:

If any user has a problem either in a specific application or he/she needs to make a change, he/she has to initiate a change order request and the initiator has to justify the change request. The change order request has to be signed by the IT Head and approved by the Registrar of the University.

4.21 In conclusion:

Since developments in email and the Internet are changing rapidly, the University reserves the right to change this policy as necessary without prior notice.
Current policies pertaining to technology resources can be located on the IT website at www.bracu.ac.bd/infotech

For any comments or questions regarding this policy please contact the BRAC University Information Technology Department at: support@bracu.ac.bd or info@bracu.ac.bd

5. CHANGES TO POLICY AND DISCLAIMER

We may change this policy from time to time, and reserve the right to do so without notice. The information provided in this privacy policy should not be construed as giving business, legal or other advice, or warranting as fail proof, the security of information provided through https://mail.bracu.ac.bd
SOFTWARE LICENSING:

All software licensing for use at BRAC University has to be licensed under the name of BRAC University Registrar.

6. CONTACT INFORMATION

For questions regarding this privacy policy, please contact:

System Administrator/Manager GDLN - aminul@bracu.ac.bd

Head of IT - nalamgir@bracu.ac.bd

Registrar BRAC University - sahool.ma@bracu.ac.bd

7. Cellular Phone and Tablet Portable Computer Usage Policy

If BRAC University provides cellular telephones or Tablet Portable Computers, as approved by departmental supervisors, to full-time and part-time employees as a business tool. They may be provided to assist employees in communicating effectively with other employees and outside clients/vendors as deemed necessary. All Customer Service calls should be directed to the IT Helpdesk during the hours of 9AM to 5PM.

7.1 Purpose:

The purpose of this policy is to provide guidelines regarding the use of and responsibilities required as BRAC University cell phone user.

- Cell phones or Tablets that are purchased through the Information Technology Department are the property of BRAC University. The primary use of the device is for University-related business. Personal use of an assigned device should be occasional, for example, business related trips or emergencies. Phone bills will be monitored for any "excessive" usage. Each user will be allocated **500** peak minutes per month. Unlimited night and weekend minutes included. All excess minutes or charges will be billed to the individual and must be repaid to the University within 60 days to avoid suspension of service.

Nights	Sunday - Thursday 9:00 P.M. to 5:00 A.M
Weekend	Friday 9:00 P.M. – Saturday 5:00 A.M
Unlimited Mobile to Mobile	Any operator to any operator
Charges for Over 500 min usage	Amount in excess over 500 minutes
Text Messaging	Not Included

NOTE: Under no circumstances should the assigned cellular phone be used as a replacement for a personal cell phone or residential landline phone.

- Individuals to whom cellular phones have been provided are responsible for the security and maintenance of the phones and must promptly report any damage, theft, or vandalism to the Information Technology Department. Individuals will be responsible for the cost of replacing damaged phones, tablets and/or accessories. Devices that are lost or stolen will have to be replaced by the individual/department and a report with Public Safety or the Police

Department will have to be filed and presented to IT. These cases must be reported to the IT Department immediately so the data can be erased remotely and the device locked to prevent malicious use of the device or data.

- Safe use of the cell phone is of utmost importance. You must abide by all local laws concerning the use of cell phones while driving. A hands free device should be utilized if talking while driving; **do not text and drive.**

8. BYOD Policy:

BRAC University is still not ready for the "Bring Your Own Device" (BYOD) policy, which is usually undertaken for cloud computing services. In future, when BRAC University introduces the BYOD policy, employees/clients will be notified about this.

9. Change of policy :

BRAC University reserves the rights to revise the clauses of the IT policy as and when required and may change the policy if required for the security, protecting the University IT resources, its faculty, staff and students from electronic and legal harm resulting from improper use of information technology.

***