ASSAM DON BOSCO UNIVERSITY
Information Technology Policy Manual

Overview
The Assam Don Bosco University has developed information technology resources usage policies to extend the mission of the University and to protect the availability, integrity and confidentiality of all information technology resources in the university, whether owned or contracted.

No set of policies can address all scenarios however these policies address most common aspects in terms of usage, security, responsibilities and procedures. The University expects all users to adhere to the policies therein.

Purpose
The purpose of the IT Policy Manual of Assam Don Bosco University is to establish a framework of policies that will protect the University's IT resources and Computer Networks, achieve accountability by providing clear roles and responsibilities and to ensure that the processes within the university are consistent with applicable laws and other guidelines laid down by University or other statutory bodies.

Scope
These policies apply to all faculty and staff members, students, IT Resources Management Committee (ITRMC), IT Resources Administrators and anyone else who uses Assam Don Bosco University IT resources.

Information Technology Resources Management Committee
The University shall constitute an Information Technology Resources Management Committee to oversee the proper handling of academic, administrative and public use of the Information Technology Resources of the University. The ITRMC shall consist of a Chairperson, appointed by the Vice Chancellor of the University, a representative from each School of the University, a representative from the Administration and four IT Resource Administrators.

It shall be the responsibility of the ITRMC to ensure adherence to the policies laid down in this document and to review this document periodically and make necessary changes to ensure that it serves the purpose for which it was designed.

IT Resource Administrators
IT Resource Administrators are usually system administrators. They shall work in close collaboration with the members of the ITRMC and are responsible for implementing the guidelines laid down in this document under the direction of the ITRMC. In particular, it shall be the responsibility of IT Resource Administrators to

- install software applications on the systems of the University and ensure that the systems are kept up to date
- Take care of timely repairs to the Networks and Systems of the University
- provide physical and procedural safeguards for the IT resources of the University.
- Assign usernames and passwords and update them as required as per the guidelines of the ITRMC
- Implement monitoring techniques and procedures for detecting, reporting and investigating incidents
- perform any other activity as shall be assigned to them by the ITRMC

POLICIES
1.0 Acceptable Use
1.1 The IT resources of the University must be utilized respectfully and as authorised and designed. While utilizing University-owned IT resources, no user or administrator shall engage in any activity that violates University policy or any illegal activity under local, state, central or international law.

1.2 Users and administrators shall not engage in any activity that interrupts personal productivity or the service of any University resource. Users and administrators shall not intentionally disrupt, damage, or alter data, software, or other IT resources belonging to the University or to any other entity. This includes spreading viruses, sending spam messages, performing denial of service attacks, compromising another individual's ability to use IT resources, and performing system/network reconnaissance.

1.3 Systems available in the Computer Laboratories and in the various departments of the University shall be handled with care. Users of University systems shall not tamper with, disable, or circumvent any security mechanism, including software applications, login account controls, network security rules, hardware devices, etc.

1.4 Users shall not introduce any prohibited information technology resources that could disrupt operations or compromise the security of the University's IT resources such as

- Computers / Devices infected with malware
- Resources, like software, bit torrents, etc., involved with illegal, malicious, or negligent behaviour

1.5 National Knowledge Network

The Assam Don Bosco University is a part of the National Knowledge Network and uses the Internet connectivity provided by it. As such, faculty staff and students shall use the Internet Services provided by the University in accordance with the guidelines laid down by the MHRD for the use of the National Knowledge Network.

2.0 Access and Access Control

2.1 All University IT resources are to be managed by the ITRMC with proper implementation procedures to authorise, document and carry out various tasks such as data access privileges, creating and assigning usernames and passwords to meet the university requirements.

2.2 All University IT resources that store, process, or transmit Confidential or protected data must require usernames and passwords for access. In particular usernames and passwords are required to access the Internet and Intranet Networks and the ERP implementation of the University. Prior authorization is mandatory for access to the University's IT resources that store, process or transmit confidential or protected data.

2.3 Individual departments are responsible for developing and implementing procedures for authorizing and granting access to the IT resources within the departments and in the Laboratories of the departments.

2.4 IT Resource Administrators shall document all data access privileges, and will re-evaluate access privileges when a user's job assignment changes. When a user no longer requires data access or leaves the University for any reason, the designated ITRA shall revoke the user's access privileges. The user's supervisor shall be responsible for making appropriate and timely requests to the ITRA for the account access modification.

2.5 Individuals with access to confidential or Protected Data may not share or redistribute such date without receiving the expressed prior consent from ITRMC

2.6 Login Names and Passwords

2.6.1. Designated ITRA shall configure systems and applications to meet the following requirements to authentic users of the University IT resources that store, process or transmit confidential or protected data.

- The designated ITRA shall assign each user of the Network facilities and the ERP of the University with a unique login name as per the guidelines laid down by the ITRMC.

- Login names shall have an associated password, which is required to meet the standards for secure passwords and which are as per the guidelines laid down by the ITRMC

2.6.2. Users must not share account passwords with any other person.

3.0 Software

3.1 Installed Software

All software packages that reside on computers and networks within the University must comply with applicable licensing agreements and restrictions and must comply with the University's own acquisition of software policies.

3.2 Ownership of Software

All knowledge resources developed by faculty, staff, students or contract personnel on behalf of the University, or licensed for the use of the University are the property of Assam Don Bosco University and must not be copied for personal use, for use at home or any other location, unless otherwise specified by the license agreement.

3.3 Free and Open Source Software

All systems in the University shall use Free Operating Systems. The University encourages the use of Free and Open Source Software for the teaching, research and administrative activities of the University. However, if proprietary software is required for certain functionalities, such software should run on a free OS. In the event that an essential proprietary software does not run on a free OS, the procurement of such software shall include the procurement of Operating Systems (proprietary) which support the software.

3.4 Virus Protection

Approved virus checking systems must be deployed at all levels. Users are not authorized to turn off or disable virus checking systems.

4.0 Copyright and Intellectual Property

4.1 The widespread use of digital technologies has enabled easy access to electronic information, images, video clips, music recordings, etc. it is important to look for the copyright symbol © in all such material. All who use copyrighted material should provide a citation for an electronic source that includes the source's URL, author or site manager's name (if available and the creation or download date.

4.2 Any activity that infringes copyright-protected materials may be subject to disciplinary action.

4.3 Those who develop and use electronic course materials should be familiar with and observe appropriate rules and procedures related to the use of copyrighted materials.

5.0 Use of Official E-mail IDs

On joining employment with the University, all faculty and staff shall be provided an official e-mail ID with usernames which follow conventions laid down by the ITRMC. All official mails shall be sent and received using these official e-mail IDs. If an employee leaves employment with the university, the official e-mail ID shall be deactivated within a month of leaving employment. Hence the employee is advised to backup any necessary personal communication immediately after leaving employment. The University shall not be responsible for any loss of data due to the deactivation of the official e-mail ID as per the norm stated above.

6.0 Confidential Data and Information Security

6.1 The University prohibits unauthorized or anonymous electronic or physical access to IT resources that store, transmit, or process any of the following:

- University confidential or protected data

- Personally identifiable information and personnel data
- Financial data
- any other regulated data

6.2 Storage

6.2.1 Storage of confidential data accessed from the servers of the University shall be limited to the minimum amount, and for the minimum time required to perform the business function, or as required by law, or State or Central statutory bodies.

6.2.2 Confidential data shall not be stored on personally owned IT resources. Users of portable devices which have University confidential data stored on them shall take extra precautions to ensure the physical possession of the portable device and the protection of the University's confidential data.

6.2.3 The University's confidential or private data shall not be accessed, transmitted, or stored using public computers.

6.2.4 System administrators shall implement access controls on all IT resources that store, transmit or process confidential or protected data at least as required by the Access Control Policy (Clause 1 of this document)

6.3 Encryption

To maintain its confidentiality, Confidential Data shall be encrypted while in transit across open or insecure communication networks, or when stored on IT resources, whenever possible. Stored data may only be encrypted using approved encryption utilities. To ensure that data is available when needed each department or user of encrypted University data will ensure that encryption keys are adequately protected and that procedures are in place to allow data to be recovered by another authorized University employee.

6.4 Service Providers

All departments of the University shall ensure that third-party third-party service providers understand the University's Confidential Data Policy and protect University's Confidential Data. No user may give a Third Party access to the University's protected or Confidential Data or systems that store or process Protected or Confidential Data without permission from persons designated for the purpose by the ITRMC and a Confidentiality Agreement in place. Access to these resources must be handled as defined in the University's Access Control Policy.

6.5 Physical Security

All University departments that store, process, or transmit Confidential Data shall maintain a Security Plan that contains processes necessary to safeguard information technology resources from physical tampering, damage, theft, or unauthorized physical access. The departments shall also take steps to ensure that all IT resources are protected from reasonable environmental threats and hazards, and opportunities for unauthorized physical access.

6.6 Disposal

6.6.1 System administrators will ensure that all data stored on electronic media is permanently destroyed prior to the disposal or transfer of the equipment.

6.6.2 Confidential Data maintained in hard copy form will be properly disposed of using University-approved processes when no longer required for business or legal purposes.

6.6.3 Access to areas such as data centres, computer rooms, telephone equipment closets, and network equipment rooms will be restricted to authorized personnel only. Areas where Confidential Data is stored or processed shall be restricted to authorized personnel and access to these areas shall be logged.

7.0 Guidelines on the use of Social Media

7.1. Any message that is posted on Social Media and which might act as the “voice” or position of the University or a constituent thereof must be approved by the appropriate authority.

7.2 A university employee or student shall not post confidential or proprietary information about the University, its employees, students, or its alumni. Further, a university employee or student shall not discuss a situation involving named or pictured individuals on a social media site without their permission.

7.3 The University staff and faculty, and not the University, shall be personally responsible for the content they publish on blogs, wikis or any other form of user-generated content. The University shall not be held liable for any comment or post deemed to be copyright infringement, defamatory, proprietary, libelous, or obscene.

8.0 Risk Management and Disaster Recovery

8.1 Risk Assessment

The ITRMC is responsible for developing processes for conducting periodical risk assessments for the University’s information technology resources, especially critical and confidential data. The results of the risk assessments shall be used to determine required security improvements and appropriate levels of risk acceptance for the various IT related processes and systems of the University. Where unacceptable levels of risk are indicated, remedial measures shall be taken as soon as possible by the ITRMC in conjunction with the Director or Departmental Head.

8.2 Business Continuity Plan

8.2.1. The ITMRC shall also maintain a current, well-documented and tested Business Continuity Plan (BCP) that outlines the University’s response to unexpected events that disrupt normal business, such as system failure, network failure, failure of Internet Connectivity, vandalism, fire and natural disaster. The BCP shall be an action-based plan that takes into account the criticality of systems, applications and data. It shall also include procedures and measures to address the retrieval and protection of critical data during an emergency.

8.2.2. The Business Continuity Plan shall also outline measures that address the maintenance of essential business processes and services in the event of a disaster and the eventual restoration of normal operations.

8.2.3. The BCP shall include documented processes for annual review, testing and revision of the BCP.

9.0 Incident Response

9.1 To ensure timely and effective handling of security incidents involving IT resources, the ITMRC shall establish and document an Incident Response Plan. All University employees with IT responsibilities are responsible for understanding and following the University’s Incident Response Plan.

9.2 All suspected and confirmed security incidents, their resolution steps and their outcomes shall be documented by those directly involved. Such documentation shall be appropriately logged and archived by the ITMRC.

9.3 All incidents of lost of stolen IT resources must be reported immediately to the person(s) designated by the ITMRC.

10.0 Compliance and Enforcement

10.1 The University expects all employees, students and users to adhere to the policies stated herein.

10.2. All violations known and /or suspected must be reported to the designated members of the ITRMC. IT Resources Administrators along with a designated member of ITRMC shall examine electronic logs, access reports and track reports periodically for access control discrepancies, breaches and policy violations.

10.3. Violations will result in appropriate disciplinary measures in accordance with the guidelines laid down by the university and other statutory guidelines.

IT Policy Responsibility Hierarchy

Policy Implementation Body: IT Resources Management Committee - ITRMC

ITRMC Chairperson
↓
IT Resources Administrators
↓
Directors / HoDs
↓
Departmental Representatives
↓
Individual Users