Information Technology Policy Manual

1. Introduction

The Assam Don Bosco University (ADBU) has developed information security policies to protect the availability, integrity, and confidentiality of University information technology (IT) resources. These policies apply to all faculty, staff, and students of the University, Data Stewards (those that manage access to data and IT resources) and anyone who uses ADBU IT resources.

The University expects all employees, students and users to adhere to the policies herein. No set of policies can address all scenarios of IT security; therefore, these policies address the most common aspects of security. We cannot eliminate malevolent behavior or irresponsibility, but we can guide users and administrators toward responsible decisions and actions.

The University Registrar manages the University's information security activities working in cooperation with the Computer Science department.

In order to protect resources from threats and ensure compliance with applicable laws and industry standards, the University will manage and regulate networks and other IT resources.

All employees must immediately report lost or stolen technology resources to the University Administrative Department (+91 361 xxxxxxx), the Computer Science Department (+91 361 xxxxxxx), and the Registrar's Office (+91 361 xxxxxxx).

The University's IT resources, whether owned or contracted, will be configured to meet the requirements set forth in these policies. Agreements that involve a third party accessing or managing the University's IT resources shall comply with all of the requirements specified in these policies.

Owners of IT resources are responsible for keeping computer systems protected from activities that could compromise the confidentiality, integrity, or availability of the resources. Owners shall perform regular and timely computer maintenance, which includes, but is not limited to, installation of software patches, and updates to malware and virus protection. The automatic implementation of patches and updates at regular intervals will be utilized for all capable devices. Owners of IT resources should be aware of the business and availability requirements for their systems, and owners shall create appropriate documentation and processes to meet the requirements outlined in these policies.

The University should direct faculty, staff and students to the information security policies and discuss the impacts and outcomes of the policies for their specific areas. Upon hire, employees will sign a "Statement of Policy Acknowledgement" which will be administered and maintained by the Human Resources department.

1.1 Contact

Dr. Basil Koikara, Registrar: bkoikara@dbuniversity.ac.in / +91 XXXXXXXXXX
Dr. Y Jayanta Singh: jayanta@dbuniversity.ac.in / +91 XXXXXXXXXX
Dr. Peter Paul Hauhnar: pphauhnar@gmail.com / +91 XXXXXXXXXX

1.2 Enforcement

Violations of information security policy may result in appropriate disciplinary measures in accordance with local, state, and central laws, as well as UGC Laws and By-Laws, General Rules of Conduct for University faculty, staff and students.

For purposes of protecting the University’s network and information technology resources, the IT policy enforcers may temporarily remove or block any system, device, or person from the University network that is reasonably suspected of violating University information security policy. These non-punitive measures will be taken only to maintain business continuity and information security, and users of the University’s information technology resources will be contacted for resolution.

Any individual who suspects a violation of this policy may report it to:

- The Administrative Department (+91 361 xxxxxxx)
- The Computer Science Department (+91 361 xxxxxxx)
- The Registrar’s Office (+91 361 xxxxxxx)

2. Acceptable Use

The Acceptable Use policy applies to all users of the University's computer and network resources.

Information technology (IT) resources must be utilized respectfully and as authorized and designed. While utilizing University-owned IT resources, no user or administrator is authorized to engage in any activity that violates University policy or any illegal activity under local, state, central or international law.

Users and administrators may not engage in any activity that interrupts personal productivity or the service of any University resources. Users and administrators will 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.

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.

Users shall not introduce any prohibited information technology resources that could disrupt operations or compromise security of the University’s IT resources. The following list of information technology resources are prohibited from operating on or with ADBU’s information technology resources:

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

3. Access Control Policy

All University information technology (IT) resources that store, process, or transmit Confidential or Protected data must require usernames and passwords for access. Prior authorization is mandatory for access to the University’s IT resources that store, process or transmit Confidential or Protected Data.

Individual departments are responsible for developing and implementing procedures for authorizing and granting access to their IT resources that store, process or transmit Confidential or Protected Data.

IT policy managers shall document all data access privileges, and will reevaluate 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 Data Steward shall revoke the user’s access privileges. The user’s supervisor is responsible for making appropriate and timely requests to the Data Steward for IT resource account access modification.

Individuals with access to Confidential or Protected Data may not share or redistribute this data without receiving the expressed, prior consent of the Data Steward.

3.1 Login Names and Passwords

Data Administrators will configure systems and applications to meet the following requirements to authentic users of IT resources that store, process or transmit Confidential or Protected Data:

- Data Administrators must assign each user a unique login name.
- Login names will have an associated password, which is required to minimally meet the standards for secure password and as per University requirements.

Users must not share account passwords with any other person.

3.2 Ownership of Software

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

3.3 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 acquisition of software policies.

The University, as a requirement, permits the use of only open source Operating Systems on its electronic assets. Required or relevant application software, licensed or otherwise, must be compatible with the open source operating system.

3.4 Virus Protection

Approved virus checking systems must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

3.5 Review and Compliance

For systems where Confidential Data is stored, processed, or transmitted, Data Stewards and Data Administrators will review user access rights annually using a documented process.

Data Stewards, or their designated representatives, shall ensure appropriate procedures are documented, disseminated, and implemented to ensure compliance with this policy.

4. Data Roles and Responsibilities

Data Stewards oversee the proper handling of administrative, academic, public engagement, or research data. Data Stewards are responsible for classifying data according to the University’s data classification system, ensuring that appropriate steps are taken to protect data, and the implementation of policies and agreements that define appropriate use of the data. The Steward or his designated representatives are responsible for and authorized to:

- Approve access and formally assign custody of an information technology (IT) resource.
- Specify appropriate controls, based on data classification, to protect the IT resources from unauthorized modification, deletion, or disclosure. The Steward will convey those requirements to administrators for implementation and educate users. Controls shall extend to IT resources outsourced by the university
- Confirm that applicable controls are in place to ensure appropriate level of confidentiality, integrity and availability
- Confirm compliance with applicable controls
- Assign custody of IT resources assets and provide appropriate authority to implement security controls and procedures
- Ensure access rights are re-evaluated when a user’s access requirements to the data change (e.g., job assignment change)

Data Administrators are usually system administrators, who are responsible for applying appropriate controls to data based on its classification level and required protection level, and for securely processing, storing, and recovering data. The administrator of IT resources must:

- Implement the controls specified by the Steward(s)

- Provide physical and procedural safeguards for the IT resources
- Assist Stewards in evaluating the overall effectiveness of controls and monitoring
- Implement the monitoring techniques and procedures for detecting, reporting, and investigating incidents

Data Users are individuals who received authorization from the Data Steward to read, enter, or update information. Data Users are responsible for using the resource only for the purpose specified by the Steward, complying with controls established by the Steward, and preventing disclosure of confidential or sensitive information.

5. Data Classification Levels

Confidential Data requires the highest level of privacy and may not be released. Confidential Data is data that is protected by either:

- Legal or regulatory requirements
- Contractual agreements (e.g., Non-Disclosure Agreements)

Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

Protected / Internal Data must be appropriately protected to ensure a lawful or controlled release. Internal Information is intended for unrestricted use within the University, and in some cases within affiliated organizations such as business partners. This type of information is already widely-distributed within the University, or it could be so distributed within the organization without advance permission from the information owner.

Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages. This is all data that is neither Confidential or Public data.

Public Data is open to all users, with no security measures necessary. Public Information has been specifically approved for public release by a designated authority within each entity of the University. Examples of Public Information may include marketing brochures and material posted to internet web pages etc. This information may be disclosed outside of the University.

6. Confidential Data

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

- University Confidential or Protected Data
- Personally identifiable information (PII) and Personnel data
- Financial data
- Any other regulated data.

6.1 Storage

Confidential Data storage will be limited to the minimum amount, and for the minimum time, required to perform the business function, or as required by law and/or State/Central Data Retention requirements.

University IT resources that are used for storage of Confidential Data shall be clearly marked to indicate they are the property of ADBU. Servers that store Confidential or Protected Data shall not be used to host other applications or services.

The University prohibits the storage of encrypted or unencrypted Credit Card / Debit Card and Internet Banking data in physical or electronic form. Confidential Data may not be stored on personally owned IT resources. Users of portable devices will take extra precautions to ensure the physical possession of the portable device and the protection of the University's Confidential and Protected Data.

The University's Confidential or Private Data may not be accessed, transmitted, or stored using public computers or via email.

System Administrators shall implement access controls on all IT resources that store, transmit, or process Confidential or Protected Data, minimally supporting the requirements defined in the Access Control Policy.

Procedures

Each calendar year, Data Users who are capable of viewing, storing, or transmitting Confidential Data shall complete the Information Security Awareness Training Program.

University employees will perform monthly scans and review results in order to locate and remove PII on each computer under their control. Storage of PII on desktop or laptop computers requires:

1. Explicit permission from the Data Steward,
2. Separate accounts for all users with strong passwords required for all accounts,
3. Whole disk encryption enabled,
4. Security logging and file auditing enabled,
5. Computer firewall enabled and logging,
6. Automatic operating system patching and antivirus software updates,
7. Automatic screen lock after a period of inactivity,
8. Restricted remote access methods, such as remote desktop and file sharing.

6.2 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. In employing encryption as a privacy tool, users must be aware of, and are expected to comply with existing government regulations.

6.3 Activity Logging & Review

IT resources that store, access, or transmit Confidential Data shall automatically log activity into electronic log files. Logging includes system, network, application, database, and file activity, whenever available, and includes creation, access, modification, and deletion activity.

Log files shall be retained electronically for the duration necessary to meet the requirements defined by the state or central Data Retention schedules.

Procedures

System administrators and/or Data Stewards shall examine electronic logs, access reports, and security incident tracking reports periodically for access control discrepancies, breaches, and policy violations. Log harvesting, parsing and alerting tools can be used to meet these requirements.

6.4 Service Providers

Departments shall take steps to ensure that 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 a permission from the Data Steward 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

Each University department that stores, processes, or transmits Confidential Data will maintain a Facility Security Plan that contains the processes necessary to safeguard information technology resources from physical tampering, damage, theft, or unauthorized physical access. Departments will take steps to ensure that all IT resources are protected from reasonable environmental threats and hazards, and opportunities for unauthorized physical access.

Access to areas containing Confidential Data information must be physically restricted. In departments with access to confidential data, all individuals must wear a University-issued identification badge on their outer garments so that both the picture and information on the badge are clearly visible.

6.6 Disposal

Systems administrators will ensure that all data stored on electronic media is permanently destroyed prior to the disposal or transfer of the equipment. The steps taken for the destruction of data will follow the University procedures.

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.

Access to areas such as data centers, 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. Secure Web Application Development and Use of Official Email lists

Secure Web Application Development

Departments will ensure that development, test, and production environments are separated. Confidential Data must not be used in the development or test environments.

All applications must be tested for known security vulnerabilities prior to being placed in production and at regular intervals thereafter.

Production application code shall not be modified directly without following an emergency protocol that is developed by the department, approved by the Data Steward, and includes post-emergency testing procedures.

Web servers that host multiple sites may not contain Confidential Data.

All test data and accounts shall be removed prior to systems becoming active in production.

The use of industry-standard encryption for data in transit is required for applications that process, store, or transmit Confidential Data.

Authentication must always be done over encrypted connections. University enterprise Central Authentication Service (CAS), or Active Directory services must perform authentication for all applications that process, store, or transmit Confidential or Protected Data.

Web application and transaction logging for applications that process, store, or transmit Confidential Data or Regulated Data must submit system-generated logs periodically.

Departments implementing applications must retain records of security testing performed in accordance with this policy.

Use of Official Email lists

As part of the University’s ongoing activities to improve communication and leverage its investment in technology, University IT services created Official Email Lists to help the University conduct its business with targeted audiences. In order to ensure that faculty, staff and students would not be inundated with mass e-mailings, oversight procedures were put in place to monitor the email messages being sent via the official email lists.

The purpose of this policy is to ensure that the Official Email Lists are used in an appropriate manner and that email users are aware of the types of official lists available, the criteria to be used when communicating via the official lists, and the procedures for using the official lists.

Official Email Lists are involuntary, closed membership, moderated lists created by University IT services. These lists are intended to provide a method for addressing official University announcements to targeted populations of students (undergraduate and graduate), faculty, employees via their officially assigned University email address (Personal name). These lists are not intended as discussion (“open forum”) lists.

Subscription to these lists is based on information in either the Student database or the Human Resources database. These lists are refreshed automatically on a regular basis to ensure that membership remains current.

Official Email Lists are available for use by any University unit (department, office, center, etc.) or recognized University organization for the purpose of sending messages that pertain to university work or typical university information such as

- Normal everyday work activities of the University
- Messages concerning emergency, health and safety announcements
- Messages pertaining to matters of university-wide policy
- Messages of a timely nature having direct impact on large numbers of one or all of the following groups: University faculty, staff and students.

8. IT Security Awareness Training

ADBU maintains an Information Security Awareness Training (ISAT) program that supports the University employees’ and students’ needs for regular training, supporting reference materials, and reminders to enable them to appropriately protect University information technology resources.

Data Stewards are responsible for ensuring that any user requesting access to Confidential Data has completed the ISAT program before allowing access to that data.

The Registrar will provide periodic Information Security reminders and updates, posted on the University website and using email lists, where appropriate.

Departments shall maintain appropriate documentation of attendance/completion of the ISAT training where data security training is required by applicable regulatory standards.

9. Incident Response

The University will establish, document, and distribute an Incident Response Plan to ensure timely and effective handling of security incidents involving IT resources. University employees with IT responsibilities are responsible for understanding and following the University's Incident Response Plan.

Suspected and confirmed security incidents, their resolution steps, and their outcomes shall be documented by those directly involved. All incidents must be appropriately logged and archived.

Procedures

All incidents of lost or stolen technology resources must be reported immediately to the University Administrative Department (+91 361 xxxxxxx), the Computer Science Department (+91 361 xxxxxxx), and the Registrar's Office (+91 361 xxxxxxx).

10. Risk Management, Business Continuity and Disaster Recovery

Risk Management

The University is responsible for developing a process for conducting Risk Assessments for the University's information technology (IT) resources.

The results of the Risk Assessment will be used to determine security improvements resulting in reasonable and appropriate levels of risk acceptance and compliance for each system.

Results indicating an unacceptable level of risk shall be remediated as soon as possible, as determined by specific circumstances and the timelines decided collectively by the Registrar, Data Steward, and the Dean, Director or Department Head.

Results of all risk assessments shall be treated as Confidential Data and secured appropriately.

Procedures

Each department is responsible for ensuring that a Risk Assessment is performed biennially for each of the information technology resources in their respective areas. Risk Assessments will also be conducted when there is an environmental or operational change that may affect the security of Confidential Data.

Business Continuity and Disaster Recovery

Each University department will maintain a current, written and tested Business Continuity Plan (BCP) that addresses the department's response to unexpected events that disrupt normal business (for example, fire, vandalism, system failure, and natural disaster).

The BCP will be an action-based plan that addresses critical systems and data. Analysis of the criticality of systems, applications, and data will be documented in support of the BCP.

Emergency access procedures will be included in the BCP to address the retrieval of critical data during an emergency.

The BCP will include a Disaster Recovery (DR) Plan that addresses maintaining business processes and services in the event of a disaster and the eventual restoration of normal operations. The BCP and DR Plan will contain a documented process for annual review, testing, and revision. Annual testing of the BCP will include desk audits, and should also include tabletop testing, walkthroughs, live simulations, and data restoration procedures, where appropriate. The BCP will include measures necessary to protect Confidential Data during emergency operations.

Data Administrators are responsible for implementing procedures for critical data backup and recovery in support of the BCP. The data procedures will address the recovery point objective and recovery time objectives determined by the Data Steward and other stakeholders.

11. Resources to back up the University's IT Policies

IT Policy - Government of India
IT Policy – Government of Assam, India
IT Policy – University of Virginia, USA
IT Policy – Virginia Tech Polytechnic and State University, USA
IT Policy – University of Connecticut, USA
IT Policy – Internet Samples