बिरला प्रौद्योगिकी संस्थान
BIRLA INSTITUTE OF TECHNOLOGY
(वि० अनु० आ० अधिनियम १९५६ की धारा ३ के तहत मानित विश्वविद्यालय ‖ A Deemed to be University u/s 3 of UGC Act, 1956)
मेसरा, राँची - ८३५२१५ (भारत) ‖ MESRA, RANCHI - 835 215 (INDIA)

फोन/Phone: (EPBX) 0651-2275444/2275896,2276002/2276006 फैक्स/Fax: 0651-2275401/2276052 वेबसाइट/website: www.bitmesra.ac.in

Ref. No. GO/Estb/CSP/24-25/4504 17th January, 2025

CIRCULAR

IMPLEMENTATION OF THE CYBER SECURITY POLICY IN THE INSTITUTE

The Competent Authority has approved for implementation of Cyber Security Policy (as per attachment) in the Institute with immediate effect and for wider circulation of the same in BIT Community.

The policy have been carefully crafted and finalised in close collaboration with the ICT Cell of the Institute and C3iHub, IIT, Kanpur to address the evolving challenges and ensure a resilient cyber security posture for the Institute.

The policy outlines key measures to safeguard Institute's digital infrastructure, promote cyber security awareness among all stakeholders and mitigate potential cyber risks.

The recommended measures are in alignment with best practices in cyber security and aim to establish a robust defense mechanism across all ICT operations at this Institute.

17/1/25

Registrar

Copy to:

1. All Dean(s)/Director (IQAC)/Controller of Examination
2. All HoD(s)/In-charge(s), Academic Departments/Sections
3. Director(s)/In-charge(s), BIT Off Campuses
4. Director, University Polytechnic/BIT-STEP
5. Prof. In-charge (ICTC/CDC/Energy Management/Water Resources Management/ Central Library/TEQIP Coordinator
6. Associate Dean(s)
7. Dy. Comptroller / Dy. Finance Officer
8. Dy. Registrar(s) / Administrative Officer (E&HR)
9. Medical Officer In-charge/Assistant Registrar(s)
10. P. S. to Vice Chancellor
11. File

SECURITY POLICY

The Institute relies intensely on information and information systems in the pursuit of its organizational objectives. If vital information were unavailable, unreachable or disclosed to inappropriate persons, the Institute could suffer loss of reputation or financial damage.

To sustain and enhance the enviable reputation that the Institute enjoys, the Executive Management of the Institute has initiated and continues to support an information security effort to manage both its information and information systems.

The definition and details of the information security policies contained in this document are a step in this direction.

To be effective, information security must be a team effort and shall involve the participation and support of every individual of the Institute, who deals with information or information systems. To bolster team work, the policies in this document clarify the responsibilities of users as well as the steps they must take to help protect the Institute's information and information systems.

This document describes ways to prevent and respond to a variety of threats to the information and information systems, including unauthorized access, loss, misuse and denial of use.

Every individual from the Institute, irrespective of status or designation must comply with the information security policies in this document. Persons who deliberately violate this and other information security statements are liable to face disciplinary action, up to and including termination. The Institute also reserves the right to injunctive relief if it deems necessary.

The various provisions in the policy have been drafted to make them in alignment with ISO 27001 standards, ISMS (Information Security Management System) guidelines and the prevailing best industrial practices.

1. Introduction

The Institute's information systems, and the information and data they contain, are fundamental to the Institute's daily operations and future success. The Institute shall implement procedures and controls at all levels to protect the **confidentiality, integrity & availability of** information stored and processed in its systems and ensure that the information is available only to authorized persons as and when required according to the business requirement.

1. Information system security policy document

This document provides the framework to ensure the protection of the Institute's information assets, and to allow the use, access and disclosure of such information in accordance with appropriate standards, laws and regulations as applicable to the Institute.

All existing Institute policies related to personnel, administration, protection of confidential information, and other areas shall apply equally to the information systems environment.

2. Information system security policy coverage

The security policies and standards contained in this document have been established to cover information and data, software, hardware and networks used by the Institute at the Main Campus and its Off-Campuses.

This policy applies to all individuals who have access to the University's IT resources, including but not limited to computers, networks, software, data, and electronic communications systems. It applies to all devices connected to the University's network, whether owned by the University or personally owned.

- All proprietary information that belongs to the Institute
- Personnel information relating to the employees of the Institute
- All customer information held by the Institute
- All supplier, contractor and other third party information held by the Institute
- All hard copy documents held by the Institute
- All software assets such as application software, system software, development tools and utilities
- All physical assets, such as computer equipment, communications equipment, media and equipment relating to facilities
- All services, such as power, lighting, HVAC associated with the Institute's information systems.

3. Objectives of Information system security policy

The overall objective of the 'Information System Security Policy' is to provide guidance and direction for the protection of the Institute's information systems against accidental or deliberate damage or destruction.

The specific objectives of the 'Information System Security Policy' are:

- Alignment of information security with business strategy to support organizational objectives.
- Alignment of information security with Academic strategy to support organizational objectives.
- Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level.
- Management of performance of information security by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved.

- Optimization of information security investments in support of organizational objectives.
- To prevent unauthorized disclosure of information stored or processed on the Institute's information systems (Confidentiality)
- To prevent unauthorized accidental or deliberate alteration of information (Integrity)
- To prevent unauthorized accidental or deliberate destruction or deletion of information necessary for operations (Availability)
- To ensure that the data, transactions, communications or documents (electronic or physical) are genuine (Authenticity)
- To ensure that a party to a transaction cannot deny having received or having sent an electronic record (Non- repudiation)
- To ensure that all the subjects with access to the information assets of Institute are identified, authenticated, authorized, accountable and auditable (Identification, Authentication Authorization, Accountability and Auditability)

The policy shall also provide guidance to the Institute that its information systems comply with relevant laws and regulations and international standards on information security management such as ISO 27001.

4. Responsibility for Information security

All employees, external contractors, Students, Faculty members and other third parties including outsourced agencies, who require access to the Institute's information systems, shall be responsible for ensuring that the information system security policies are adhered to and that they operate systems in such a manner to ensure its security.

- Management at all levels shall be responsible for ensuring that staff are aware of, and adhere to, this policy and the standards.
- The IT department shall provide guidance on Implementation of the Security Policy but the responsibility will be entirely of the respective asset owners. .

5. Ethics in the field of security

The basis for security consists of the shared ethical norms and attitudes relating to ownership, and the respect for each other and each other's possessions that are shared at the work place. It is ethical to:

- As management, clarify prevailing rules
- As a user of Institute's IT resources who could be employee, student, faculty member or a third-party employee respect the Institute's possessions and resources, and make sure that they are used correctly.
- Protect sensitive or confidential information

It is unethical to:

- Actively study information one has gained access to by mistake
- Spread information that can in some way hurt others / and the Institute's interest
- Actively hide one's identity
- Appropriate authority or rights in excess of those granted
- Make private statements or publish private material in the name of the Institute
- Sharing of user-ids until strictly required and formally authorized.

6. Scope of the policy document

The policy document shall be organized un the following sections:

- The International Standard: ISO 27001 Code of Practice defines Information Security as the preservation of three aspects of Information:
  - **Confidentiality**: Information is only available to those that are authorised to gain access.
  - **Integrity**: Safeguarding the accuracy and completeness of information and processing methods.
  - **Availability**: The assurance that authorised users have access to information and associated assets when this is required.
- Information System security policy framework
- Security violations
- Information System security policy statements

The policy is applicable to

- All staff (permanent & on contractual basis) and non-employees (contractors, consultants, suppliers, vendors etc.), Students and Faculty members of the Institute and other individuals, entities or organizations that have access to the Institute's IT systems.
- All locations where users have access to various IT Assets and IT Services including locations that have secure areas providing critical IT Assets and IT Service
- All IT Assets and IT Services involving data, applications, network, security devices, servers and other IT system that needs to be appropriately protected from physical and environmental threats
- All Service Provis who rent their IT services to the Institute and have access to the Institute facility.

7. Distribution of the policy document

1. The Information System Security policy is a confidential document and is meant for permitted use. Such permissions shall be accorded by the IT head.

2. Every person in custody of the document has the responsibility for ensuring its confidentiality. The custodian of the document shall ensure that the document is regularly updated with amendments that may be issued from time to time.

2. Access Control Policy

1. Objective

Access control policy has been designed to help system and network administrators to decide on the level of access required by a user and assign the rights and permissions accordingly

2. Policy

1. Access control matrix at the Institute should be designed to facilitate users in their work environment and at the same time control their access to the IT systems/facilities.

2. All users are assigned rights and permissions based on the requirements of the roles and responsibilities they hold to perform their duties at the Institute.

3. Separate access control matrix should be maintained for the employees and the vendors/business partners.

4. Respective System Administrator/s should create the user account, as per 'User Management Policy' and rights and permissions should be assigned as per the Access Control Matrix.

5. Respective System Administrator/s should be informed about the changes in user work profile due to promotion, transfer etc.

6. Respective System Administrator/s should carry out the required changes in the Access Control Matrix and update the rights and permissions assigned on the IS/IT system.

3. User Management Policy

1. Objective

User Management Policy aims at assisting the System Administrators in carrying out user account management tasks including – user account creation/deletion, maintenance of user accounts, defining and maintaining user access privileges, etc.

2. Policy

1. User Account Creation/Deletion

1. All users requiring access to the Institute's network should be assigned unique user accounts and passwords.

2. Respective department/functional heads should be responsible for informing the respective System Administrators about the user account creation for any third party vendor, business partner or any other such entity requiring temporary access to the Institute Network Systems.

3. User account creation/deletion form should be filled and approval taken from the respective System Administrator for this purpose.

4. Respective System Administrator should be responsible for user account creation/deletion and maintaining the records for all the user accounts created/deleted from the IS/IT systems of the Institute.

5. All the user accounts created and maintained on the Institute's IT systems should follow a standard naming convention.

2. User Account Maintenance Guidelines

1. All default user accounts on various systems, in use at the Institute, should be renamed, wherever feasible.

2. All the vendors, business partners, temporary employees/trainees should be assigned user accounts with least access privileges and should have limited validity period.

3. On the last day of work for any employee leaving the organization, all the accounts associated with that employee should be disabled/deleted from the IT systems deployed across the Institute's network.

3. Password Guide Lines (to be implemented wherever feasible)

1. Strong passwords are long, to be more 8 characters
2. There is at Least One Upper Case and One lower Case Character
3. There is at least One Special Character
4. There is at least One Number (numeral)
5. Use Multi Factor Authentication (MFA) wherever possible.

4. Procedure for User creation

1. New user creation for New Employee

1. Once the resource confirms the joining date, the Institute's respective Department and its identified resource for this, will initiate his/her login credentials.
2. Department resource will send an email to IT Team.

2. Disabling of user-ID for Exiting Employee

1. The respective department shall be responsible for disabling the user id, well in time, of the impending exit of the employee.
2. On receipt of this information from the Department, the IT team shall disable the Institute email account pertaining to the employee.
3. However, depending on the gravity of the case, if the employee is being terminated on disciplinary grounds the concerned employee's user-ID and email account shall be disabled immediately.
4. The respective department shall inform the IT team about the particulars of the employee as soon as possible.

3. New User ID Creation on OS, Database and Application

1. New user IDs will be created after a review and approval process.

4. Management & Review of Access Rights

1. All users should be provided least access rights on a need to know basis. The Access rights of Privileged and VPN Users should be performed every six months and access should be extended only after continued Business need is established.

4. Anti Virus Policy

1. Objective

Anti-virus policy of the Institute aims at creating and maintaining a virus-free work environment.

2. Policy

1. Anti-Virus Solution Installation

1. The Institute should use a single corporate standard anti-virus solution.

2. Windows based Desktops, Laptops and Servers should have Anti-Virus installed.

2. Anti-Virus Logging and Reporting

1. Periodic reports should be generated and reviewed by the Security Administrator and appropriate actions should then be taken.

2. Any virus outbreak or related issue should be reported to and addressed through the IT Department.

3. Updating Virus Definition Files

1. Anti-virus solution at the Institute should support common updates for anti-virus patterns for all the modules and application where anti-virus software is deployed.

2. Updated virus definition files should be downloaded from the vendor's site on a regular basis and the users informed about the availability of the same.

3. Antivirus Administrator should be responsible of updating the virus definition.

5. Security Logging and Monitoring Policy

1. Objective

System logging and Monitoring policy aims at detecting unauthorized activities being performed or any such attempt of unauthorized access. Logging of security-relevant activities and configure alarms for suspicious security events.

2. Policy

1. All production systems within the organization shall record and retain audit-logging information that includes the following information.

2. Audit Logging should be enabled on All Servers, Network Devices, Databases, Applications and Privileged User Activity

3. Logs of critical systems should be reviewed periodically using Security Information & Event Management (SIEM) solution with 24x7 monitoring within 12-18 months of the Launch of this Policy.

   Initially OS and Network logs can be integrated along with Application-level logs wherever technically feasible.

4. Mechanism for Automated review of Logs and prompt incident Response should be explored.

5. Storage of Logs - The Logs should be stored for a period of 2 years for the purpose of Review and Forensics. The logs can be online or in Archived format. All logs should be available online for at least 30 days time.

6. Network Management Policy

1. Objective

Network Management policy outlines the activities to be performed by the IT department and the network controls that should be put in place and followed by the users.

2. Policy

1. Network Administration

1. IT systems, Network and telecommunication controls should be deployed at the Institute to protect critical and business sensitive information from unauthorized and illegal access through network and communication links.

2. Network Administrator should be responsible for the administration of the corporate network from a central location.

3. Network administrators should also be designated at various locations and should regularly review the network configurations and take adequate measures to provide physical, logical and procedural safeguards for its security.

4. Network Administrator should maintain a list of personnel from the IT team, vendors and others who can access the routers and other network devices including security devices.

5. Automated alert and notification system should be deployed at the critical systems to inform network administrator if there is any possible breach of network security like unauthorized access, hacking or virus infection or any other event that hinders the operations at the respective system.

6. Administrative privilege to all the routers should be provided to the Network Administrator only or the appropriate persons.

2. Connectivity

1. If the business requirement arises, connectivity from other networks and computer system with corporate network must be approved and documented.

2. All unused connections and network segments should be disconnected from active networks.

7. Backup Policy

1. Objective

Backup policy has been devised to provide guidelines to the users and the IT department for the purpose of backing up data and systems as per the requirements of the Institute.

2. Policy

1. Backup

1. The users and Administrator should jointly ensure the availability and reliability of the data/information when and where required by taking regular backups.

2. List of Critical Devices or Applications will be maintained by IT Team.

3. Backup for the identified Devices and Applications will be performed by the respective owners, as per procedure laid down by the IT Team.

4. All the backup activities should be logged and a backup register should also be maintained.

5. Backup should be stored on Multiple Cloud Location or Physical Media. If stored on Physical Media adequate controls of Labelling & safe storage should be implemented.

2. Testing the backup

1. Backup Administrator should be responsible for periodically testing the data backed up.

2. Data and system files that are backed up should be tested once every six months.

3. Any discrepancies or errors found during the backup testing should be reported to the IT Head and to the concerned departmental head.

4. The test results should be documented and the backup process modified to avoid similar discrepancies in future.

3. Backup Frequency

1. One time backup

1. Systems software loaded on the Institute server(s) should be backed up and stored so that the downtime of server is maintained at the minimum level.

2. Backups should be updated as and when any change or update patch is applied to the system.

2. *Scheduled Backup*

1. Backup activity should be performed as per the guidelines of the IT department.

8. System Acquisition and Development Policy

1. Objective

System acquisition policy is developed with the objective of providing standard guidelines to be followed in case of procurement/development of Hardware systems/Packaged software.

2. Policy

1. Acquisition of Hardware/Software

1. Security and Compliance requirements as per Security Policy should be included in the RFP and Purchase of any Hardware or Software procured by the Institute.

2. If there is any Non-compliance noted at procurement stage of any Hardware/Software, the same should be recorded and due management approvals would be required, if such a Solution is Procured to address any critical Business requirements.

2. In-house Software Development

For the in-house Software developed principles of Secure Software Development Life Cycle should be followed, where the Security Requirements are embedded and addressed in every phase of the Software development Life Cycle.

The Software Development Life Cycle at has following Phases:

1. *Requirement Analysis*

   Security Requirements will be incorporated in the Requirements Phase.

2. *Design*

   Design should incorporate the Security requirements to develop Secure and robust Software.

3. *Implementation & Coding*

   IT department would provide guidance on following best practices in Software Development activities. Any security vulnerabilities identified during testing would be remediated before moving the code to production.

   Steps should also be taken to ensure that the deployment can be done in an automated manner to minimize any human errors as far as possible.

4. *Testing & UAT*

   Software developed should be tested for Security Vulnerabilities and risks identified should be remediated before the Code can be transferred to production.

5. *Production & Maintenance*

   Only Security Tested Software should be allowed to go live in Production unless management level approval has been taken. With the application of suitable compensatory controls till such a time the identified risks are remediated.

9. Physical and Environmental Security

1. Objective

The Institute's Physical and Environmental policy intends to ensure that all the High Security areas are adequately guarded to avoid any physical intrusion and to ensure equipment safety in case of any unforeseen happening.

2. Policy

1. Physical Access Controls

1. Physical access controls through appropriate Lock and Key arrangement, CCTV monitoring etc should be provided in sensitive and critical areas, wherever possible.

2. No eatables should be allowed at workplace. Provision for cafeteria/canteen should be made for consuming eatables.

2. Logging of Physical Access

All the visitors, whether employees, vendors or one-time visitors, should record their entries to the sensitive and critical areas in the visitor's logs/Register. The records should include the time of entry, personnel visited, purpose of visit and the time of exit.

3. Equipment Security

1. Provisions should be made to supply adequate power supply to all the IT equipment/facilities. Specifications for the same should be sought from the respective vendor.

2. All the assets should be covered under comprehensive insurance to provide cover for any monetary loss that the Institute might suffer due to unforeseen occurrences.

10. Data Classification Policy

1. Objective

The purpose of this policy is to provide a set of guidelines, for protecting Data and Assets that are critical to the Institute. Users who may encounter any data or classified information or Assets are expected to familiarize themselves with this policy.

2. Policy

1. Data Classification and Control

Data and information generated and processed at the Institute, by the virtue of its operations, is confidential and sensitive. Depending on the business criticality, the Institute classifies its data in two categories of 'Critical' and 'Non-critical'.

Data classification should follow uniform classification labelling. All the data/information generated and in use should be categorized and classified as –

1. *Critical*

   Data used for running the business operations like Finance, Marketing, and Research etc.

   List of Critical Data would be maintained and updated regularly in consultation with Data Owners, Management Team and members of IT Team. The primary responsibility will be of the Data owner.

2. *Non-critical*

   Data that is not critical and is an extra aid in the decision-making process is categorized as 'Low' criticality information.

3. *Sensitive*

   Any Research Data, Academic Record or Students / Employee / Vendor Data which is considered Sensitive should be identified and treated separately.

2. Additional Controls

Additional controls would need to be identified and implemented for the Sensitive and Critical Data.

11. Asset Classification and Control

1. Objective

Asset classification policy aims at guiding the employees with identification of Information and Data assets that should be secured to create a secure environment.

2. Policy

1. Classification Labeling and Inventory of Assets

The Institute should classify its IS/IT systems/facilities used for storing and processing Business data as 'Critical' and 'Normal'. All the IS/IT assets should be categorized and classified as:

1. *Critical*

   All IT assets that store and process business critical data and information, including the daily transactions, are categorized as 'Critical' systems. Systems that should be consied in this category should include – application Servers, Database Server, Firewall Systems, Security Administration Systems, Domain Server, Web Server, Networking Solutions, Mail Server, Proxy Server etc.

2. *Normal*

   All IT assets that store and process information that is not critical as well as not so important and is an extra aid in decision making process are categorized as 'Normal' systems.

2. Additional Control

Additional controls would need to be identified and implemented for the Critical assets.

3. Asset Inventory

The inventory of all the IS/IT assets should be maintained and updated as per the requirements.

4. Secure Media Transfer and Storage

The Media used for Backup which is in physical format will be stored in a Secure place and adequate controls will be put in place during transfer of any such media.

5. Asset & Data Disposal

All Assets, once obsolete, can be disposed off only after ensuring that the Data stored in them is cleaned. Guidelines for Disposal of old assets should be established.

12. Vulnerability Management Policy

1. Objective

The vulnerabilities in IT Infrastructure, Web Applications & Mobile Applications account for the largest portion of attack vectors.

It is crucial that Vulnerabilities in the IT Landscape are assessed and are remediated on a regular basis.

A key objective of the organization's Information Security Program is to focus on detecting information security weaknesses and vulnerabilities so that incidents and breaches can be prevented wherever possible.

2. Policy

1. **Inventory of IT Assets** covering Servers, Network Equipment, Web & Mobile Applications (Internally developed and externally procured or Partner Applications) will be maintained and an updated Inventory would be maintained Every Six months of the Year, based on feasibility.

2. **Vulnerability Management Program** would be Rolled out for IT Assets as per updated Inventory List every Six Months and the Identified Vulnerabilities are remediated adopting a Risk based approach.

3. **List of Exceptions** would be maintained and updated, where it is not possible to immediately remediate ALL vulnerabilities. The Exceptions can be permanent or for a Limited duration through Approvals from Management Representative, authorized to grant such approvals, upon the request of IT Team.

4. **Regular Vulnerability Testing** will be performed on a Six Monthly basis and a Governance mechanism will be established to Track closure of Vulnerabilities and associated Risk Mitigation.

5. All security issues that are discovered during assessments must be mitigated based upon the following risk levels. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

6. All **New Applications & Assets would be Tested** for Vulnerabilities before they go live in Production for the first time and would be subsequently included in the Asset Inventory list for Quarterly Vulnerability Scanning.

13. Clean Desk Policy

1. Objective

A clean desk policy can be a crucial tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation.

The purpose for this policy is to establish the minimum requirements for maintaining a “clean desk” – where sensitive/critical information is secure in locked areas and out of site.

2. Policy

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area.

2. Computer workstations must be locked when the workspace is unoccupied.

3. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

4. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

5. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

6. All printers and fax machines should be cleared of papers as soon as they are printed.

14. Disaster Recovery Policy

1. Objective

The primary goal continuity plan is to ensure critical IT operations to continue in emergency/disaster conditions, by introduction of appropriate strategies and recovery steps.

The objectives of a Disaster Recovery Plan (DRP) are to minimize financial and operational loss of reputation and business in event of a disaster or calamity. The Institute should be able to continue to carry out its operations, mitigate the negative effects disruptions can have.

2. Policy

1. IT Disaster Recovery Plan

1. **Identify the Location of Critical Data and Assets** Identify the Critical Assets, associated data and locations whose function needs to continue or resume operations within specified period.

2. Document detailed set of processes, procedures and activities which need to be carried out during disaster scenarios.

3. Roles and responsibilities of each member should be documented and communicated to the respective members who are supposed to participate during the operationalisation of the Disaster Recovery Plan.

4. There should be a detailed communication plan consisting of who would be announcing the disaster, which departments are impacted, the target audience and list of stakehols who should be informed of the disaster should be reviewed every six months

15. Secure Configuration & Hardening Policy

1. Objective

Hardening is the process of securing a system by reducing its surface of vulnerability by ensuring Secure Configuration. The aim is to reduce the number of vectors of attack by the removal of any unauthorized software, removal user accounts or services that are not required for planned system functions.

2. Policy

1. For Software or Network Devices used in the IT Landscape, secure configurations would be implemented before release into production. This would be applied to every product and its version from any vendor.

2. Effort should be made to ensure that All Operating Systems, Subsystems, Databases, Network Devices are configured per Security Guidelines maintained by IT department as far as possible.

3. List of Software generally used will be maintained by each department. Advisory should be given by the department head to not install any other software without appropriate approvals.

4. Disable or Remove Unnecessary Usernames

5. Accounts relating to services or functions which are not used should be removed or disabled.

6. For all accounts which are used the default passwords should be changed.

7. Only software that has been approved for use by the IT department may be installed on the organization's computing devices.

8. All PC's, Servers, Cloud Resources and laptops will be built from a standard image. Any change to the standard image must be supported by a business case.

16. Acceptable Usage Policy

1. Objective

Acceptable Usage Policy (AUP) outlines the acceptable use of the Institute's information technology resources and systems by all stakeholders, including students, faculty, staff, contractors, and guests.

The purpose of this policy is to ensure the integrity, availability, and confidentiality of the University's IT resources while promoting responsible and ethical use.

2. Policy

1. **Authorized Use**
   1. IT resources provided by the University are to be used for authorized academic, administrative, research, and other University-related activities.
   2. Users must comply with all applicable laws, regulations, and University policies when using IT resources.

2. **Security**
   1. Users are responsible for safeguarding their accounts, passwords, and access credentials. Sharing accounts or passwords is strictly prohibited.
   2. Users must not attempt to circumvent or disable security measures or gain unauthorized access to IT resources.
   3. Users must report any suspected security breaches or incidents promptly to the appropriate University authorities.

3. **Data Protection and Privacy**
   1. Users must respect the privacy and confidentiality of data stored on University systems.
   2. Unauthorized access, use, or disclosure of sensitive or personal information is strictly prohibited.
   3. Users must comply with applicable data protection laws and University policies regarding the collection, use, and retention of data.

4. **Intellectual Property**
   1. Users must respect copyright and intellectual property rights when accessing or sharing information through University IT resources.
   2. Unauthorized usage, distribution or sharing of copyrighted materials is prohibited.

5. **Responsible Use**
   1. Users must refrain from engaging in activities that may disrupt or degrade the performance of IT resources or interfere with the

activities of others.
2. Offensive, harassing, or discriminatory behavior in electronic communications or online activities is prohibited.
3. Users must not use IT resources for illegal, unethical, or fraudulent purposes.

6. **Network Usage**
   1. Users must comply with the University's network usage policies, including bandwidth limitations and restrictions on peer-to-peer file sharing.
   2. Unauthorized installation or use of network devices that may compromise the security or integrity of the network is prohibited.

7. **Social Media and Online Presence**
   1. Users representing the University on social media or other online platforms must adhere to the University's social media guidelines and branding standards.
   2. Users must exercise caution and professionalism in their online interactions, respecting the reputation and values of the University.

17. Software Licensing and Open-Source Software Usage Policy

1. Objective

Software Licensing and Open-Source Software Usage Policy outlines guidelines for the acquisition, use, and distribution of software within the University. It aims to ensure compliance with software licensing agreements, promote responsible software usage, and encourage the appropriate adoption of open-source software.

2. Policy

1. **Software Acquisition and Licensing**
   1. All software acquisitions must be made in compliance with applicable licensing agreements and copyright laws.
   2. Only authorized personnel are permitted to acquire software licenses on behalf of the University.
   3. Prior approval must be obtained for any software purchases or license agreements, and purchases must be made through approved procurement channels.

2. **License Compliance**
   1. Users must adhere to the terms and conditions of software licenses, including restrictions on installation, usage, and distribution.
   2. Unauthorized duplication or distribution of software is strictly prohibited. Users must promptly report any unauthorized or unlicensed software installations to the appropriate university authorities.
   3. The Asset Owner would be solely responsible for any penalty or punitive action is any unlicensed is identified and would be liable for the appropriate disciplinary action as deemed fit by Institute.

3. **Open-Source Software Usage**
   1. Open-source software may be used within the University, subject to compliance with applicable open-source licenses.
   2. Users must review and understand the terms of open-source licenses before deploying open-source software.
   3. Proper attribution must be provided for any open-source software used or distributed by the University.

4. **Approval Process**
   1. Department heads would publish a list of software authorized for use by the Team every six months.
   2. Prior to adopting new software, users must conduct a thorough evaluation to assess its suitability, security, and compliance with university policies.
   3. All software acquisitions and deployments must be approved by the appropriate departmental or administrative authority.