Digital Personal Data. Protection (DPDP) Act, 2023

Naipunnya Institute of Management and Information and Technology (NIMIT)

1. Introduction

Cyber Security is the intricate practice of protecting systems, mobile devices, data, networks, and programs from cyber-attacks, or any unauthorized access. These attacks aim at accessing, amending, leaking or destroying secret information or interrupting smoothly running business processes. As cyber-attacks are increasing with an increase in digitization in our society, implementing effective cyber security measures is the need of the hour.

Our Cyber security measures:

1. Anti-Virus: Seqrite endpoint security offers a comprehensive platform which integrates innovative technologies like Anti Ransom ware, Advanced DNA Scan, and Behavioural Detection System to protect our networks from advanced threats.
2. Firewall: Sophos XG Firewall protects our network from ransom ware and advanced threats including top- rated IPS, Advanced Threat Protection, Cloud Sandboxing and full AI-powered threat analysis, Dual AV, Web and App Control, Email Protection.

The Information Technology and Knowledge Management (IT) Policy of Naipunnya Institute of Management and Information Technology (NIMIT) establishes a framework for the secure, ethical, and effective use of Information and Communication Technology (ICT) resources within the institution. This policy ensures that all academic, administrative, and research activities leverage technology responsibly while safeguarding institutional and personal data. It is designed in alignment with:

- **AICTE and UGC Guidelines** for IT infrastructure and digital learning.
- **Ministry of Electronics & Information Technology (MeitY)** governance and cyber security framework.
- **Indian IT Act (2000) and its amendments**, including Data Protection and Privacy principles.
- **Digital India and NEP 2020** initiatives to promote technology-enabled education.

By adhering to this policy, the institution fosters a secure digital environment that supports academic excellence, research, innovation, and administrative efficiency.

3. Objectives

The primary objectives of this IT Policy are to ensure that Information & Communication

Technology (ICT) resources of NIMIT are used responsibly, securely, and effectively to enhance academic, administrative, and research excellence. Specifically, the policy aims to:

3.1 Ensure reliable, secure, and cost-effective use of IT resources

- Provide uninterrupted and reliable access to computing, networking, and internet facilities.
- Optimize bandwidth usage to prioritize academic and research needs over non-academic activities.
- Implement cost-effective procurement, licensing, and maintenance of IT assets (hardware, software, cloud services).
- Establish IT disaster recovery and business continuity mechanisms.

3.2 Promote digital teaching, learning, and research

- Encourage the use of digital libraries, e-resources, and virtual labs to supplement classroom teaching.
- Facilitate online collaboration through secure video conferencing and research-sharing platforms.
- Provide access to high-performance computing, simulation software, and research databases.
- Encourage innovation, hackathons, and use of AI/ML/IoT platforms in line with emerging technologies.

3.3 Safeguard institutional and personal data

- Protect sensitive student, faculty, and administrative data using encryption and secure access controls.
- Enforce strict data backup, archival, and retention policies.
- Prevent unauthorized data sharing, cyber threats, and breaches through firewalls, IDS/IPS, and endpoint security.

3.4 Support compliance with Govt. of India initiatives

1. Align institutional IT practices with **Digital India** initiatives, including paperless administration, e-governance, and digital literacy.
2. Incorporate **National Education Policy (NEP) 2020** recommendations by promoting online learning, blended learning, and technology-enabled pedagogy.
3. Follow **CERT-In cyber security guidelines** and conduct regular awareness programs on safe digital practices.
4. Promote adoption of **open-source software** where feasible, in line with Govt. of

India's open standards framework.

4. Scope

This IT Policy is **institution-wide** in nature and applies to all individuals and ICT resources associated with Naipunnya Institute of Management and Information Technology (NIMIT). It ensures that every stakeholder uses technology responsibly, securely, and in compliance with national standards.

4.1 Applicability – Users

The policy applies to:

1. **Faculty Members** – teaching and non-teaching staff using institutional IT facilities.
2. **Administrative Staff** – office staff, finance, HR, and examination personnel using digital systems.
3. **Students** – undergraduate, postgraduate, students accessing academic IT resources.
4. **Research Scholars** – Ph.D., scholars using computing facilities.
5. **Visiting Faculty, Alumni, and Guests** – when granted temporary access to campus IT resources.
6. **Vendors, Contractors, and External Partners** – who are provided access to networks, data, or systems for official purposes.

4.2 Applicability – IT Assets

The policy covers all ICT resources owned, leased, or managed by the institution, including:

1. **Networking & Connectivity** – Internet, intranet, Wi-Fi, VPN, routers, firewalls, switches, and servers.
2. **Computing Devices** – desktops, laptops, workstations, tablets, smartphones, and IoT devices connected to institutional networks.
3. **Storage & Data Systems** – databases, file servers, NAS devices, and cloud storage platforms (Google Workspace).
4. **Software & Applications** – licensed, open-source, institution-developed, and third-party applications.
5. **Audio-Visual Equipment** – projectors, smart boards, video conferencing tools, and digital classrooms.
6. **Security & Surveillance Systems** – CCTV, biometric systems, access control systems, and monitoring software.

4.3 Geographical & Access Scope

This policy applies to both **on-campus** and **off-campus** access, including:

1. Campus buildings, laboratories, libraries, and hostels.

2. Mobile access from personal devices (BYOD – Bring Your Own Device), subject to institutional security controls.
3. External collaborations with universities, industries, or research bodies using college IT infrastructure.

5. IT Infrastructure Usage Policy

5.1 Network & Internet Usage

The institution's network and internet facilities are provided primarily for **academic, research, and administrative purposes**. To ensure secure and fair usage, the following guidelines apply:

5.1.1 User Access Control

1. Network and Wi-Fi access shall be provided only through **authorized credentials** (faculty, staff, student, or guest IDs).
2. All users must authenticate themselves using **unique login IDs and passwords** assigned by the IT Department.
3. **Guest/Visitor access** will be provided only upon approval by the IT Administrator with restricted privileges.
4. Use of personal hotspots, unauthorized routers, proxy servers, or repeaters is strictly prohibited.

5.1.2 Internet Usage Monitoring

1. All internet traffic (browsing, downloads, uploads, emails) is **logged and monitored** as per **CERT-In and Govt. of India cyber security guidelines**.
2. Internet access shall comply with applicable laws, including the **Indian IT Act (2000)** and subsequent amendments.
3. Users are prohibited from accessing websites or online services that are illegal, harmful, or unrelated to academic/research activities (e.g., pornography, gambling, piracy, extremist content).
4. Peer-to-peer file sharing (e.g., torrents) and excessive streaming (OTT, gaming) may be restricted to conserve bandwidth.

5.1.3 Bandwidth Management

1. Internet bandwidth is considered a **shared institutional resource** and shall be allocated based on academic and research priorities.
2. Bandwidth-intensive activities (e.g., research data transfer, virtual labs, online learning platforms, digital library access) shall take precedence over recreational use.

3. Bandwidth limits (quotas) may be imposed on users or departments to prevent misuse.

5.1.4 Network Security

1. The network will be protected using **firewalls, intrusion detection/prevention systems (IDS/IPS)**, and web filtering mechanisms.
2. End-user devices connecting to the network must have **up-to-date antivirus and OS patches**.
3. Unauthorized scanning, hacking, or probing of the network is strictly forbidden and will be treated as a **cybercrime**.
4. Any attempt to bypass institutional security controls (VPN tunneling, proxy circumvention, spoofing) is prohibited.

5.1.5 Responsibilities of Users

1. Users must not share their login credentials with others.
2. Users are responsible for all activities carried out under their account.
3. Any suspicious or unauthorized network activity must be reported immediately to the IT Department.
4. The institution reserves the right to **suspend or revoke access** in case of misuse, policy violation, or security threat.

5.2 Email & Communication Policy

The institution's official email system is an essential medium for academic, administrative, and research communication. To ensure professionalism, security, and effective use, the following guidelines apply:

5.2.1 Official Email Accounts

1. All **faculty, staff, and students** shall be provided with an official institutional email ID (e.g., @mkce.ac.in) hosted on authorized platforms such as **Google Workspace (G Suite for Education)** and **Microsoft 365 (O365 Education)**.
2. The official email ID must be used for all **college-related communication** including academic activities, research correspondence, administrative notices, and external collaborations.
3. Use of **personal email accounts (Gmail, Yahoo, etc.)** for official communication is discouraged and may be restricted for sensitive transactions.

5.2.2 Bulk Email and Mass Communication

1. Academic or administrative announcements (e.g., exam notifications, circulars, seminar invites) should use **designated mailing lists** managed by the IT team.

2. Unauthorized mass emails or promotional content is strictly prohibited.

5.2.3 Acceptable Use

1. Email accounts must be used **professionally** and strictly for academic, research, and administrative purposes.
2. Sending **spam, phishing links, hoaxes, chain mails, or offensive/abusive content** is prohibited.
3. Users must not impersonate others or misrepresent their identity in email communication.
4. Use of email for **political, religious, or commercial solicitation** unrelated to institutional activities is strictly disallowed.

5.2.4 Email Security

1. Users must protect their email credentials by following **strong password policies** (minimum length, complexity, periodic change).
2. Enabling **multi-factor authentication (MFA/2FA)** is strongly recommended for all official accounts.
3. Suspicious emails (phishing attempts, malware attachments) must be reported immediately to the IT Department.
4. The institution reserves the right to **scan emails** for viruses, malicious attachments, and spam, in compliance with data protection laws.

5.2.5 Retention, Backup & Monitoring

1. Institutional emails may be **archived and backed up** periodically for legal, academic, or administrative purposes.
2. The IT Department will maintain **logs of email usage** as per **CERT-In guidelines** and Govt. of India cyber security requirements.
3. In case of disciplinary investigations, relevant email records may be accessed by authorized authorities after due approval.

5.2.6 Termination of Accounts

1. Email accounts will be **deactivated** upon completion of a student's course or faculty member's/non-teaching member's resignation/retirement of staff.
2. Alumni or retired staff may be provided with **limited access accounts** (with storage restrictions) if approved by management.

5.3 Hardware & Software Policy

The institution is committed to ensuring that all computing devices and software are **secure, legal, and well-maintained**. The following guidelines govern the use of

hardware and software resources:

5.3.1 Hardware Usage

1. All desktops, laptops, projectors, biometric devices, and servers purchased by the institution must be **registered with the IT Department**.
2. Users must not tamper with institutional hardware, modify configurations, or attempt unauthorized repairs.
3. Any **addition or removal** of IT equipment (e.g., lab systems, laptops, printers) must be recorded in the **IT Asset Register**.
4. Hardware disposal (e-waste) must comply with **Govt. of India E-Waste Management Rules, 2016**.
5. Personal devices (BYOD – Bring Your Own Device) connected to the institutional network must comply with college security requirements (antivirus, patches).

5.3.2 Software Licensing

1. Only **licensed and approved software** may be installed on institutional systems.
2. Installation or use of **pirated, cracked, or unauthorized software** is strictly prohibited.
3. Software purchased under academic/research licenses must not be used for **Commercial purposes**.

5.3.3 Installation & Updates

1. All software installations must be carried out or approved by the **IT Department/IT Administrator**.
2. Regular **operating system updates** and **security patches** must be applied to all devices.
3. Approved **antivirus and endpoint protection tools** must be installed and updated on all systems.
4. Unauthorized installations of games, entertainment applications, peer-to-peer sharing tools, or hacking utilities are prohibited.

5.3.4 Asset Security & Configuration

1. All computers must be configured with **standard security settings** (firewall enabled, auto-update turned on).
2. Faculty and staff laptops should be password-protected and encrypted if handling sensitive data.
3. Lost or stolen institutional devices must be reported immediately to the IT

Department.

4. IT staff reserve the right to **inspect and audit devices** connected to the institutional network for compliance.

5.3.5 User Responsibilities

1. Users are responsible for the **proper care** of the devices assigned to them.
2. Users must not install, remove, or alter licensed software without IT approval.
3. Any malfunctioning system must be reported to the IT Helpdesk; self-repair attempts are discouraged.
4. Violation of this policy may lead to **suspension of IT access** and disciplinary action.

5.4 Data & Storage Policy

The institution recognizes **data as a critical asset** and is committed to ensuring its confidentiality, integrity, and availability. This policy governs the storage, management, and protection of all academic, administrative, and research data.

5.4.1 Authorized Storage Platforms

1. Institutional data must be stored only on **authorized platforms** such as **Google Workspace (G Suite for Education)**, **Microsoft 365 (OneDrive/SharePoint)**, or institution-managed servers.
2. Use of **personal storage accounts (Gmail Drive, Dropbox, external USB drives, etc.)** for official data is discouraged and may be restricted for sensitive data.
3. Cloud platforms must comply with **Govt. of India data residency and privacy guidelines**.

5.4.2 Data Classification

All institutional data shall be classified into:

1. **Public Data** – information meant for public access (e.g., brochures, website content).
2. **Internal Data** – academic schedules, notices, non-sensitive administrative documents.
3. **Confidential Data** – student records, examination papers, payroll, HR files, research proposals.
4. **Restricted/Sensitive Data** – financial records, legal documents, health data, and government-mandated sensitive information.

5.4.3 Confidential & Administrative Data

1. Confidential data (student details, examination records, staff payroll, etc.) must be

encrypted both in transit and at rest.

2. Access to such data shall follow the **principle of least privilege** – only authorized staff should have access.
3. Critical administrative data must be backed up regularly in **secure offsite or NAS storage**.
4. Any sharing of confidential data outside the institution requires **written authorization** from management.

5.4.4 Research Data Management

1. Research data generated through projects, consultancy, or funded programs must be stored and maintained in line with the **funding agency's Data Management Policy** (AICTE, UGC, DST, DBT, SERB, etc.).
2. Large datasets, simulations, and experimental results must be stored on **secure institutional servers or approved cloud repositories**.
3. Research involving sensitive data (healthcare, personal information, etc.) must comply with **ethical clearance** and **DPDP Act 2023** provisions.
4. Upon project completion, data must be archived and retained as per sponsor/funding guidelines.

5.4.5 Backup & Recovery

1. All critical academic and administrative data must be **backed up periodically** (Daily/weekly depending on sensitivity).
2. Backups must be stored in **secure, access-controlled environments** (separate physical servers).
3. A **Disaster Recovery Plan (DRP)** shall be maintained to restore operations in case of hardware failure, cyber-attacks, or natural disasters.

5.4.6 Data Retention & Disposal

1. Student, staff, and administrative records must be retained for the duration specified by **UGC/AICTE/University regulations**.
2. Expired data must be securely deleted using **data wiping or destruction methods** to prevent recovery.
3. E-waste containing storage media (hard disks, SSDs, pen drives) must be disposed of as per **E-Waste Management Rules, 2016**.

5.4.7 User Responsibilities

1. Users must not store unauthorized or pirated files (movies, games, copyrighted material) on institutional storage.
2. Users must ensure **strong passwords** and avoid sharing access credentials for shared drives.
3. Faculty, staff, and researchers are responsible for **periodic review and clean- up** of their allocated storage.
4. Any data breach, accidental loss, or unauthorized access must be **reported immediately** to the IT Department.

5. Cyber security & Privacy Policy

The institution is committed to safeguarding its digital infrastructure, academic resources, and personal data of stakeholders (students, faculty, staff, and research collaborators). All cyber security measures align with **CERT-In guidelines, AICTE/UGC norms, the Indian IT Act 2000 & its amendments, and the Digital Personal Data Protection (DPDP) Act 2023**.

5.1 Password & Authentication Policy

1. Users must create strong passwords of **minimum 8–12 characters**, including uppercase, lowercase, numbers, and symbols.
2. Passwords must be changed at least **once every 90 days** and should not be reused.
3. Multi-Factor Authentication (MFA/2FA) must be enabled wherever supported (e.g., email, LMS, ERP).
4. Sharing of passwords is strictly prohibited. If compromised, users must reset immediately and report to the IT Department.

5.2 IT Systems Security

1. Institutional IT infrastructure (servers, firewalls, routers, switches) shall be secured with **enterprise-grade firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and endpoint protection software**.
2. All computers and devices must run **updated antivirus/antimalware software** approved by the IT Department.
3. Regular **security patches and firmware updates** shall be applied to all systems.
4. Remote access to the network must only be via **secure VPNs** approved by the IT Admin.

5.3 CCTV & Physical Security

1. CCTV surveillance will be deployed across critical areas (campus entry/exit, data

centers, exam sections, labs).

2. CCTV footage shall be **retained for a minimum of 30–90 days** (as per Govt. of India and UGC norms) and securely stored.
3. Access to CCTV recordings will be limited to authorized personnel only.
4. CCTV usage will comply with **privacy and ethical guidelines**, ensuring footage is not misused.

5.4 Data Privacy & Protection

1. Collection, processing, and storage of personal data (student records, staff files, and health data) must comply with the **DPDP Act 2023**.
2. Consent must be obtained from individuals before collecting or sharing their personal data.
3. Only **minimum necessary data** will be collected and retained.
4. Data shall be anonymized or pseudonymized for research purposes where feasible.
5. Data transfers to third parties (vendors, agencies, research partners) require **Data Processing Agreements (DPAs)**.

5.5 Compliance & Monitoring

1. IT systems will be subject to **regular security audits, penetration testing, and vulnerability assessments**.
2. Logs of network activity, system access, and email communications will be maintained as per Govt. of India norms.
3. Any violation of cyber security policies may result in suspension of IT privileges, disciplinary action, and legal proceedings under the **Indian IT Act 2000/DPDP Act 2023**.

6. Research & Innovation Policy

The institution supports **cutting-edge research, innovation, and entrepreneurship** by providing access to advanced IT infrastructure, promoting open knowledge, and safeguarding intellectual property rights.

6.1 Use of Software & Tools

1. Faculty, research scholars, and students are encouraged to use **open-source software** (e.g., GNU/Linux, R, Python, Scilab, Octave, LaTeX) where feasible, to reduce costs and promote collaboration.
2. Proprietary/licensed software (e.g., MATLAB, AutoCAD, Ansys, SPSS) may be used where necessary, in compliance with institutional licensing agreements.

3. Unauthorized or pirated software installations are strictly prohibited.

6.2 Data Management in Research

1. Research data must be stored securely in **institution-approved repositories, encrypted drives, or authorized cloud services**.
2. Confidential and sensitive data (patents, industry collaborations, human subject research) must follow **data protection norms** and **ethical committee approvals**.
3. Funding agency guidelines (DST, DBT, AICTE, UGC, SERB, international collaborations) on **data retention, sharing, and reporting** must be strictly followed.
4. Wherever applicable, **open data principles** (FAIR – Findable, Accessible, Interoperable, and Reusable) should be encouraged.

6.3 Innovation & Entrepreneurship Support

1. The institution encourages students and faculty to engage in **startups, hackathons, incubators, and innovation challenges** using institutional IT resources.
2. Access to **prototyping labs, IoT labs, AR/VR labs, robotics labs, and 3D printing facilities** shall be provided under supervision.
3. IT infrastructure used for entrepreneurship must be for **authorized innovation activities** only, not for personal or commercial gain without institutional approval.

6.4 Intellectual Property Rights (IPR)

1. All research outputs, software, and innovations developed using institutional resources must comply with the **institutional IPR Policy** and the guidelines of the **IPR Cell / Innovation Council (IIC)**.
2. Patents, copyrights, and trademarks shall be filed as per institutional norms, with due credit to inventors.
3. Any collaboration with **industry partners or external agencies** must include clear agreements on **ownership, revenue sharing, and IP licensing**.
4. Researchers must respect copyright laws and avoid plagiarism, data manipulation, or unethical publishing practices.

6.5 Responsible Research & Ethics

1. All research must comply with **ethical standards set by UGC, AICTE, and institutional ethics committees**, particularly for human and animal studies.
2. Plagiarism checks (using Turnitin /Urkund or equivalent) are **mandatory** for all

theses, dissertations, and publications.

3. Use of AI, big data, and analytics in research must be conducted with **Transparency, fairness, and accountability**.
4. International collaborations must comply with **Government of India regulations on cross-border data sharing and research partnerships**

7. Social Media & Digital Conduct Policy

The institution recognizes social media as a powerful tool for communication, collaboration, and outreach. However, its misuse can harm the **reputation of the college, faculty, and students**, and may result in legal or disciplinary action.

7.1 Professional Conduct Online

1. Faculty, staff, students, and research scholars are expected to maintain **Professionalism and decorum** in all online interactions.
2. Users must not engage in **hate speech, bullying, harassment, discrimination, or defamatory remarks**.
3. Political campaigning, spreading misinformation, or promoting extremist views using institutional IT resources is strictly prohibited.
4. All online communication must reflect the **values of respect, inclusivity, and academic integrity**.

7.2 Official Institutional Social Media Accounts

1. Only **designated staff members or the Public Relations/Media Cell** may create, manage, or post content on the **official social media handles** of the institution (Facebook, Twitter/X, Instagram, LinkedIn, YouTube, etc.).
2. Content published on official accounts must:
    1. Be accurate, professional, and aligned with institutional objectives.
    2. Avoid confidential or sensitive information.
    3. Comply with **AICTE, UGC, and Govt. of India communication guidelines**.
3. Unauthorized creation of accounts or use of the college name/logo for unofficial pages is prohibited.

7.3 Personal Social Media Usage

1. Faculty, staff, and students are free to use personal social media accounts outside institutional platforms, but they must not:
    1. Misrepresent themselves as official spokespeople of the institution.
    2. Share confidential academic/administrative/research data without

approval.

3. Use institutional email IDs for creating non-academic personal accounts.

2. When identifying themselves as part of the institution, users must include a disclaimer:

   "Views expressed are personal and do not represent the official position of Naipunnya Institute of Management and Information Technology (NIMIT) ."

7.4 Use of Social Media for Teaching & Research

1. Social media may be used for **academic discussions, networking, knowledge sharing, and outreach**.
2. Faculty may use platforms like **LinkedIn, ResearchGate, GitHub, YouTube, or academic blogs** for educational purposes.
3. Students must obtain **faculty approval** before creating project-related pages, YouTube channels, or blogs using institutional identity.

7.5 Cyber security & Legal Compliance

1. All social media activities are subject to **Indian IT Act 2000, DPDP Act 2023, and relevant cyber laws**.
2. Users must not post or share:
   1. Copyrighted material without permission.
   2. Fake news, misinformation, or unverified claims.
   3. Content that may lead to **defamation, legal liability, or institutional reputational damage**.
3. The institution reserves the right to monitor and take disciplinary/legal action against violations.

7.6 Digital Well-being & Responsible Usage

1. Students and faculty are encouraged to practice **digital well-being**, avoiding overuse of social media during academic hours.
2. Awareness programs on **cyber ethics, online safety, and responsible digital citizenship** will be conducted annually.
3. Any instance of **cyberbullying, online harassment, or digital misconduct** must be reported to the **IT Cell / Anti-Ragging Committee / Grievance Cell** for redressal

8. IT Governance & Administration

The institution shall establish a structured **IT governance framework** to ensure accountability, compliance, transparency, and efficient management of ICT resources.

8.1 IT Policy Committee

The **IT Policy Committee** shall be the apex decision-making body for IT-related governance.

Composition:

Chairperson: Principal / Director

Members: Director IT, HoD IT, Department (HoD's), Administrative Officer

Student Representatives: Nominated from UG/PG/Research Scholars

Ex-officio Members: Coordinator of Research & Innovation Cell, IQAC (Internal Quality Assurance Cell) representative

Responsibilities:

- Formulate, review, and update the IT Policy annually.
- Ensure alignment with **AICTE/UGC guidelines, NEP 2020, MeitY frameworks, and cyber security norms (CERT-In, NIC, NCIIPC)**.
- Approve IT infrastructure procurement and vendor contracts.
- Monitor IT budget allocation and utilization.

8.2 IT Administration

1. Daily IT operations shall be managed by the **IT supporting staff**, reporting to the IT-Head.
2. Responsibilities include:
    1. Network, server, and cloud administration.
    2. Hardware and software lifecycle management.
    3. User account management (faculty, staff, student credentials).
    4. Security monitoring, patch management, and endpoint protection.
    5. Providing IT support through a **helpdesk/ticketing system**.

8.3 IT Audits & Compliance

1. Regular audits ensure accountability and performance:
    1. **Internal IT Audits**: Conducted every 6 months by the IT Cell/IQAC.
    2. **External IT Audits**: Conducted annually by certified third-party auditors.
2. Audits shall cover:
    1. Cyber security and data protection compliance.
    2. Network performance and uptime monitoring.
    3. Software licensing and asset management.
    4. User access and privilege management.
3. Audit reports shall be reviewed by the IT Policy Committee and corrective actions implemented.

8.4 Disaster Recovery & Business Continuity

1. The institution shall maintain a **Disaster Recovery Plan (DRP)** and **Business Continuity Plan (BCP)**.
2. Measures include:
    1. Regular data backups (onsite and offsite/cloud).
    2. Redundant servers and network systems for critical services.
    3. Emergency response protocols for cyber-attacks, natural disasters, or power outages.
    4. Periodic drills to test recovery and continuity readiness.

8.5 Monitoring & Reporting

1. The IT Cell shall maintain logs of:
    1. Internet activity, firewall events, access control, and data backups.
    2. System uptime, incident reports, and helpdesk resolution statistics.
2. The **IT Head** shall submit a **quarterly IT performance and compliance report** to the Principal/Director and IQAC.
3. Major incidents (cyber breaches, data leaks, outages) must be reported immediately to the **Principal, CERT-In, and relevant regulatory authorities**.

9. Enforcement & Penalties

The IT Policy is binding on all users of ICT resources at Naipunnya Institute of Management and Information Technology (NIMIT). Violations of this policy will result in disciplinary and/or legal action, depending on the severity of the offense.

9.1 Principles of Enforcement

1. Enforcement will follow the principles of **fairness, transparency, and proportionality**.
2. Users will be given an opportunity to explain or appeal against reported violations.
3. Disciplinary actions will be consistent with institutional **Code of Conduct, HR rules, Student Regulations, and AICTE/UGC norms**.

9.2 Types of Violations

Minor Violations:

1. Sharing passwords or leaving systems unsecured.
2. Excessive personal use of institutional IT resources during academic hours.
3. Unintentional breach of software/hardware usage policy.

Moderate Violations:

4. Unauthorized installation of software or use of pirated applications.
5. Circumventing network security measures (e.g., VPN misuse, rogue Wi-Fi access points).
6. Misuse of official email/social media for spam, harassment, or offensive content.

Severe Violations:

7. Unauthorized access (hacking, privilege escalation).
8. Data theft, leakage of confidential academic/administrative/research data.
9. Cyberbullying, online harassment, or dissemination of hate speech.
10. Use of IT resources for illegal or criminal activities (cyber fraud, piracy, extremist propaganda).

9.3 Disciplinary Actions

Depending on the nature and severity of the violation, actions may include:

Verbal or Written Warning (for minor violations).

Restricted Access – Temporary suspension of internet, email, or system access.

Suspension – Denial of IT privileges for a fixed duration; in case of students, restriction from LMS/online exams.

Disciplinary Action – As per institutional rules:

1. For Students: Reporting to HoD/Disciplinary Committee → penalties, suspension, or expulsion.
2. For Faculty/Staff: Reporting to Principal/HR → penalties, suspension, or termination.

Legal Reporting – For severe breaches:

3. Incident reported to **CERT-In (Indian Computer Emergency Response Team)**.
4. Filing of complaints with **Cyber Crime Police / Indian IT Act 2000 / DPDP Act 2023**.
5. Co-operation with law enforcement agencies for investigation.

9.4 Escalation Matrix

First Level: IT Cell reviews incident and applies initial measures (warning/restriction).

Second Level: Escalation to **HoD / IT Policy Committee** for moderate/severe cases.

Third Level: Principal/Director and Governing Council decide on final disciplinary action.

Legal Level: Cybercrime cases reported to CERT-In and Cyber Crime Police, as mandated by Govt. of India.

9.5 Appeals & Grievances

Users have the right to appeal against disciplinary actions within **7 working days** of notification.

Appeals will be reviewed by the **IT Policy Committee and Grievance Redressal Cell**.

Decisions of the Principal/Director shall be final and binding.

9.6 Record Keeping & Transparency

All violations, investigations, and disciplinary actions will be documented and maintained by the IT Cell.

Annual compliance and violation summary will be submitted to the **IQAC/NAAC/ISO committee** for review.

10. Review & Update

To ensure relevance, compliance, and effectiveness, the IT Policy of Naipunnya Institute of Management and Information Technology (NIMIT, will undergo systematic review and periodic updates.

10.1 Review Cycle

The IT Policy shall be **reviewed at least once every academic year** by the **IT Policy Committee**.

Extraordinary reviews may be conducted in response to:

- New guidelines from **AICTE, UGC, NBA, NAAC, or Ministry of Education**.
- Policy directives from the **Ministry of Electronics & IT (MeitY), CERT- In, or NCIIPC**.
- Changes in legislation such as amendments to the **IT Act 2000, DPDP Act 2023**, or other cyber security laws.
- Emerging technology trends (AI, IoT, Cloud, 5G, etc.) that impact institutional ICT use.
- Major cyber security incidents or audit recommendations.

10.2 Review Process

Step 1: IT Cell conducts a compliance check and gathers feedback from faculty, staff, students, and administrators.

Step 2: Draft revisions are prepared and circulated to all stakeholders.

Step 3: The **IT Policy Committee** finalizes the updated draft.

Step 4: Approval obtained from the **Principal/Director and Governing Council**.

Step 5: Updated version published on the college website, LMS, and circulated via official email.

10.3 Version Control & Documentation

Each policy revision shall be assigned a **version number, date of approval, and review cycle**.

Archived copies of previous versions will be maintained by the **IT Cell / IQAC** for reference and audit purposes.

A **Change Log** will record all modifications with details of the section updated, reason for change, and approving authority.

10.4 Stakeholder Communication & Training

All users (faculty, staff, students, researchers) will be informed of updates via **Email, notice boards, and orientation programs**.

Awareness/training sessions will be conducted after each major update to ensure compliance.

10.5 Responsibility for Updates

The **IT Admin / IT - Head** and **IQAC Coordinator** shall jointly oversee the review and update process.

The **Principal/Director** holds final approval authority for any amendments.

****