REGIONAL INSTITUTE OF PARAMEDICAL AND NURSING SCIENCES ZEMABAWK: AIZAWL

IT POLICY

IQAC DOC NO- 40

1. **Introduction**

1.1. This Information Technology (IT) Policy outlines the principles and guidelines for the acceptable use, security, and management of IT resources and digital assets at the Regional Institute of Paramedical and Nursing Sciences (RIPANS). It applies to all faculty, staff, students, and third parties accessing RIPANS IT infrastructure.

2. Purpose of the IT Policy

2.1. The IT Policy is designed to establish guidelines for the proper, secure, and lawful use of the IT infrastructure provided by the institution. Its primary objective is to safeguard the confidentiality, integrity, and security of the college's information assets. These assets include computer systems, network equipment, software, intranet and internet services, IT devices, software applications, and all other hardware and software resources associated with IT services.

3. **Objectives**

3.1. Ensure secure, efficient, and effective use of IT systems

3.2. Protect institutional data and digital assets

3.3. Define acceptable and prohibited uses of IT resources

3.4. Promote a culture of cybersecurity awareness and responsibility

3.5. Encourage e-governance to increase efficiency, transparency, and accessibility, and reduce costs.

4. **Scope**

4.1. This policy applies to all RIPANS campuses, departments, and affiliated entities, including all users who access or manage institutional IT systems and data.

5. **Ownership and Governance**

5.1. All IT policies are governed and maintained by the Director RIPANS in coordination with IT Team and other functional departments.

6. **Acceptable Usage Policy**

6.1. IT resources are for institutional purposes only.

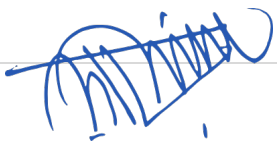
6.2. Personal use should be minimal and must not interfere with institutional duties.

6.3. Users must not engage in any activity that compromises network security or institutional reputation.

6.4. All users must comply with software licensing and copyright regulations.

7. Hardware and Software Procurement and Maintenance Policy

7.1. All computer systems across the campus will be managed by IT Team.



7.2. All IT equipment will be procured with an active warranty, and upon expiration, systems will be maintained under a structured Annual Maintenance Contract (AMC) in collaboration with authorized distributors and vendors.

7.3. Maintenance services include reinstallation of operating systems, virus scanning, bandwidth usage monitoring, resolving internet outages, repairing communication cable faults, UPS system monitoring, firewall renewals, antivirus updates, hardware replacements, software upgrades, and upkeep of licensed software.

7.4. Each department will be equipped with desktop computers or laptops featuring HD cameras, Dolby Digital audio, internet access, and printers. These facilities will be designated for departmental faculty use, who are responsible for proper utilization and compliance. All equipment will be procured based on departmental requests, approved through a multi-tier process involving the Head of Department/Principal, Director, and financial authorities. Repairs and replacements will be managed by external service providers under AMC.

7.5. All computing and networking equipment will be powered via UPS units to prevent disruptions. Web servers will be provided with uninterrupted 24/7 power through rechargeable battery systems, which undergo routine maintenance.

7.6. During installation, careful planning ensures that network cables will be laid separately from electrical wiring to minimize data transmission interference. Network infrastructure will be regularly monitored, with weekly inspections by IT Team to maintain performance standards and ensure operational integrity across the campus.

8. Software Installation Policy & Licensing

8.1. Licensed software will be used in all institutional systems, with licenses may be renewed periodically. Hardware with pre-installed licensed operating systems may be purchased.

8.2. Licenses for application software will be properly maintained and renewed on a regular basis to ensure that all applications remain valid and up to date.

8.3. Software usage across the campus will be actively monitored by the IT Team to evaluate the effectiveness and utilization of licensed applications.

8.4. The institute shall strive to promote and encourage the effective use of open-source software solutions.

9. Network (Intranet & Internet) Usage Policy

9.1. Internet will be provided for institutional functions. Non-work-related use must not disrupt operations.

9.2. The IT Team will devise an appropriate technique to allocate, secure, and monitor the internet usage by an individual.

9.3. The IT Team will be responsible for overseeing and maintaining both internet and intranet services across the campus.

9.4. Prohibited activities include hacking, unauthorized downloads, and accessing inappropriate content.

9.5. RIPANS administration reserves the right to filter or block websites deemed inappropriate based on content and associated risks.

9.6. The IT Team shall maintain an up-to-date, detailed network architecture diagram, with access granted strictly on a need-to-know basis to authorized personnel.

9.7. The wireless network infrastructure shall be logically separated from the wired LAN and strengthened with robust authentication mechanisms, encryption, detection of rogue devices, and appropriate physical safeguards.

10. Wi-Fi Usage Policy

10.1. The campus shall be fully Wi-Fi enabled, offering comprehensive wireless coverage.

10.2. Wireless access points will be installed throughout the main and annex buildings, covering classrooms, seminar halls, labs, staffrooms, and administrative offices.

10.3. Students will also be granted Wi-Fi access for academic use.

10.4. Additional access points will be installed as per growing demand and evolving requirements.

10.5. Guest users, including visiting speakers and resource persons, will be provided temporary access upon request.

10.6. Firewall configurations and website access restrictions will be enforced to maintain network security and responsible usage.

10.7. All wireless Access Points and Base Stations connected to the RIPANS network must be registered and receive approval from the Director RIPANS.

11. Clear Desk and Screen Policy

11.1. Users must lock or log off from systems when away.

11.2. Confidential materials should be securely stored when not in use.

11.3. Passwords must be kept confidential and changed periodically.

11.4. Unattended equipment must be secured against unauthorized access.

12. Workstation Usage Guidelines

12.1. Respective staff are accountable for the computers and devices assigned to them and are responsible for ensuring adherence to these policies.

12.2. Only the IT Team may perform hardware or software modifications.

12.3. Systems must be regularly updated with patches and antivirus software.

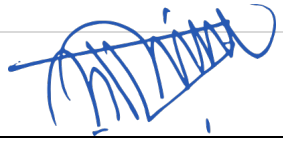
12.4. Incidents like data loss or system compromise must be reported immediately to the IT Team.

13. Printer Usage

13.1. Printing must be limited to official purposes.Users must dispose of sensitive prints securely.

14. Email Usage

14.1. Upon joining the institution, faculty and staff members will be provided with an official email username and password by IT Team with the approval of the Director RIPANS.



14.2. Principal/ HODs and coordinators and administrative staff shall receive an additional set of credentials. The official institutional email format will be:*Faculty/Staff* – *username@ripans.ac.in*

14.3. LMS access will be provided to all faculty, students, and staff.

14.4. Email will serve as an official channel of communication.

14.5. Faculty may use electronic tools for course delivery and communication.

14.6. Personal email accounts should not be used for institutional correspondence.

14.7. Spam and suspicious emails must be reported to the IT Team.

14.8. Users required to use their official RIPANS e-mail accounts for all communications with external parties and RIPANS team members.Similarly, whenever possible, emails should be sent to recipients' official institutional e-mail addresses rather than personal ones.

14.9. Upon an employee's resignation or termination, the user's e-mail account must be promptly deactivated following written order from RIPANS administration. This responsibility lies with the RIPANS IT team.

14.10. Users are accountable for all data sent, received, or forwarded through their institutional e-mail accounts.

14.11. The following types of email communications are strictly forbidden when using the official email system:

14.11.1. Containing defamatory, offensive, racist, obscene, or harassing content

14.11.2. Intended to intimidate or harass others.

14.11.3. Send chain letters, political messages, or for personal entertainment purposes.

14.11.4. Transmit copyrighted materials, software, or any legally protected information without proper authorization.

14.11.5. Transmission of proprietary, confidential, privileged, or sensitive information.

14.11.6. Containing sexual content, pornography, or any material deemed lewd or highly inappropriate in the context of official institutional communication.

14.11.7. Messages that violate any applicable laws, including copyright regulations, or go against institutional policies.

14.11.8. Emails knowingly containing malicious software, such as viruses.

14.11.9. Misrepresentation of the sender's identity or impersonation of another individual.

14.11.10. Accessing or attempting to access another person's email account without explicit authorization.

15. Student Usage Policy and Responsibilities

15.1. Sharing passwords or any other confidential information is strictly forbidden.

15.2. Students must use computers in all laboratories responsibly and with due care.

15.3. Unauthorized access to another user's personal or private data is not permitted.

15.4. Downloading, distributing, or using copyrighted institutional materials—including music, movies, software, or textbooks—without prior authorization is strictly prohibited.

15.5. Students are not allowed to access restricted institutional resources without appropriate permissions.

15.6. Students are expected to follow ethical computing practices, demonstrate academic integrity, and use shared resources judiciously.

15.7. Downloading or accessing inappropriate, unethical, or offensive content, such as obscene images or videos, is strictly prohibited and will result in disciplinary action.

15.8. Students must regularly check Learning Management System (LMS) and RIPANS website for official communication.

16. **Video Surveillance Policy**

16.1. Closed-Circuit Television (CCTV) systems will be installed across most areas of the institution to ensure safety and security.

16.2. Video footage will be monitored routinely to maintain a secure environment.

16.3. Access to the Surveillance Control Room will be strictly restricted to authorized personnel.

16.4. Video recordings may be shared upon formal request and only with prior approval from the Director RIPANS.

16.5. CCTV cameras shall undergo regular maintenance to ensure proper functioning.

16.6. Live video feeds will be overseen by the Principal/HoD, and Administrative Head.

17. Institutional Web Hosting Policy

17.1. The RIPANS website may be hosted through a third-party service provider or developed and maintained in-house, depending on institutional requirements and available resources.

17.2. Departments, Sections, or Divisions Supplying Information for website content updates must be approved by Director RIPANS.

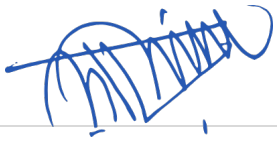
17.3. A website updating committee shall be constituted to update the contents on the institution's website.

18. Commercial Use

18.1. The use of IT resources for commercial or promotional purposes—such as advertisements, solicitations, or other messaging—is strictly prohibited unless explicitly authorized.

19. IT Asset Management

19.1. IT Team will establish clear procedures for the effective management of hardware and software assets.



19.2. These procedures will cover all stages of the asset lifecycle, including procurement, deployment, maintenance, usage tracking, energy audits, and responsible disposal of IT resources within the institution.

20. **Firewall and Network Security**

20.1. Firewalls, antivirus systems, and secure configurations must be implemented.

20.2. All networks must be protected by content filters and intrusion prevention systems.

20.3. Firewalls must block unauthorized traffic.

20.4. Configuration changes must require approval and follow a change management process.

20.5. Network components must be logically segmented and documented.

20.6. Regular audits and backups of firewall configurations will be mandatory.

20.7. All inbound and outbound traffic that does not align with RIPANS' institutional objectives will be blocked by default.

20.8. The RIPANS IT Team is responsible for maintaining an up-to-date firewall access rule set.

20.9. Firewalls must be protected with strict physical access controls to prevent unauthorized handling.

20.10. Logical access to firewalls shall be restricted and granted only with proper IT Team authorization.

20.11. Firewalls must be securely configured with hardening measures to reduce vulnerabilities.

20.12. Firewall logs will be retained for one month (or longer as per internal client requirements) in accordance with RIPANS' log retention matrix.

20.13. These logs must be regularly reviewed, and any anomalies or suspicious activities should be promptly recorded and investigated.

20.14. Firewall configurations must be backed up daily, as defined in the 'Backup' section of the Operations Security Policy.

20.15. Any changes to firewall settings must follow the formal Change Management process and be properly authorized.

20.16. Firewalls must protect all critical applications from both internal and external threats.

20.17. Firewall configurations shall allow access only to authorized users and only to approved network services.

21. **Policy Compliance**

21.1. All users must comply with this policy. Violations may lead to disciplinary actions, including termination of access, suspension, or legal actions as applicable.

22. **Review and Update**

22.1. The RIPANS IT Policy will be reviewed annually or as needed to accommodate technological or institutional changes.