# IT POLICY

# Table of Contents

# IT POLICY

## 1.1 NEED FOR AN IT POLICY

- The University's IT Policy exists primarily to maintain, secure, and ensure the legal and appropriate use of the information technology infrastructure established by the University on the campus.
- This policy establishes University-wide strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by this policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

Undoubtedly, intranet and internet services have become the most important resources in educational institutions and research organizations. Realizing their importance, MRDU took the initiative in 2015 and established the basic network infrastructure in the academic complex of the University.

Over the last five years, not only have the active users of network facilities increased manyfold, but the number of web-based applications has also grown significantly a welcome development in the University's academic environment.

At present, the University has about 1,620 network connections covering more than nine buildings across the campus, and this number is expected to reach 2,500 connections very soon.

The **Internet Unit** is the department responsible for managing the University's intranet and internet services. It runs the firewall security, proxy, DHCP, DNS, email, web, and application servers and manages the entire University network.

MRDU currently receives its Internet bandwidth from **Vainavi**, with a total availability of **500 Mbps**.

## 1.2 CHALLENGES IN PROVIDING INTERNET ACCESS

While educational institutions provide Internet access to their faculty, students, and staff, they face certain constraints:

- Limited Internet bandwidth.
- Limited infrastructure such as computers and laboratories.
- Limited financial resources for providing network facilities to faculty, students, and staff.
- Limited technical manpower for network management.

On one hand, resources are not easily available for expansion to accommodate the continuously rising Internet demand; on the other, uncontrolled, uninterrupted, and unrestricted web access can give rise to activities unrelated to teaching, learning, or governance of the University.

At the outset, it is necessary to recognize the problems related to uncontrolled Internet use:

- Prolonged or intermittent surfing affecting the quality of work.
- Heavy downloads that choke the available bandwidth.
- Exposure to legal liability or sexual-harassment issues due to harmful or offensive content.
- Leakage of confidential information into the public domain.

## a) Network Performance Issues

With extensive Internet usage, network performance suffers in several ways:

- Compared to the speed of the Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) becomes a potential bottleneck.
- When users have unrestricted access to the Internet, non-critical downloads can clog the network, resulting in poor Quality of Service (QoS) and affecting critical users and applications.
- When computer systems are networked, viruses entering through the Internet/Intranet spread rapidly, exploiting operating-system vulnerabilities.

Too many concurrent users on high-speed LANs accessing the Internet through limited bandwidth create severe strain on available resources. Every download adds to overall traffic and costs and, beyond a point, reduces the Quality of Service. Hence, reducing unnecessary Internet traffic is essential.

## b) Threats and Security Measures

Computer viruses attach themselves to files, spread quickly when those files are shared, and are often difficult to eradicate. Some can damage files or even reformat hard drives, causing extensive data loss, while others replicate silently, consuming network space and slowing down performance.

Additionally, considerable employee time is lost when infected systems require scanning and cleaning. Emails, unsafe downloads, file sharing, and web surfing are the primary causes of virus attacks. Once inside the network, viruses replicate rapidly and cause significant data damage. They can slow down or even bring the network to a complete halt.

Containing a virus once it spreads is not an easy task; it causes loss of time, data, and productivity. Therefore, **prevention** is crucial.

To secure the network, the Internet Unit has implemented multiple safeguards installing firewalls, enforcing access control, and deploying antivirus and content-filtering software at the gateway.

However, in the absence of a clearly defined IT Policy, it becomes difficult to convince users about the necessity of these controls. Users may feel that such restrictions are unwarranted or infringe on their freedom.

As IT users are aware, all educational institutions worldwide have formal IT policies in place. Without strong management policies, IT security measures may be ineffective or misaligned with organizational objectives.

Hence, policies and guidelines form the foundation of the institution's IT security program. Effective policies are essential, often required during IT audits or legal proceedings.

Policies also serve as blueprints to help the institution implement security measures. An effective security policy is as vital to a robust information-security program as a solid foundation is to a building.

Therefore, MRDU proposes to establish its own **IT Policy**, serving as a guideline for using the University's computing facilities including computer hardware, software, email, information resources, intranet, and Internet access collectively termed *Information Technology (IT)*.

This document presents proposed IT policies and guidelines relevant to MRDU's context. While designing these policies, careful consideration has been given to maintaining a balance between security and user functionality.

Due to the dynamic nature of Information Technology, information-security policies must also evolve regularly to reflect new technologies, changing requirements, and operating procedures.

The purpose of the IT Policy is to set direction and provide clarity on acceptable and prohibited actions related to IT resource use. Guidelines help departments and individuals understand how University policies apply in specific areas and promote compliance.

## 1.3 CLASSIFICATION OF IT POLICIES

IT policies are classified into the following groups:

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- Email Account Use Policy

- Website Hosting Policy
- University Database Use Policy

Further, the policies are applicable at two levels:

- **End-User Groups** (Faculty, Students, Senior Administrators, Officers, and Other Staff)
- **Network Administrators**

## Applicability

The University's IT Policy applies to:

- All technology administered by the University centrally or by individual departments;
- Information services provided by the University or any of its departments;
- Authorized individuals of the University community;
- Authorized resident or non-resident visitors using their own hardware connected to the University network.

This policy also extends to resources administered by central administrative departments such as the Library, Computer Centers, Laboratories, University Offices, recognized Associations or Unions, Hostels, Guest Houses, or Residences wherever the University provides network facilities.

Computers owned by individuals or research projects connected to the campus network are subject to the *Do's and Don'ts* detailed in the University's IT Policy.

All faculty, students, staff, departments, and authorized visitors who are granted access to the University's IT infrastructure must comply with the Guidelines.

Violations of this IT Policy by any University member may result in disciplinary action by the University authorities. If the matter involves illegal activity, law-enforcement agencies may be involved.

## Applies To

**Stakeholders (ON or OFF campus):**

- Students: UG, PG, Research
- Employees (Permanent / Temporary / Contractual)
- Faculty
- Administrative Staff (Technical / Non-Technical)
- Higher Authorities and Officers
- Guests

**Resources Covered:**

- Network devices (wired / wireless)
- Internet access
- Official websites and web applications
- Official email services
- Data storage
- Mobile / desktop / server computing facilities
- Documentation facilities (printers / scanners)
- Multimedia content

## 2.0 IT HARDWARE INSTALLATION POLICY

The University network user community needs to observe certain precautions while installing computers or peripherals so that they face minimal inconvenience due to interruptions of services caused by hardware failures.

### A. Who Is a Primary User

An individual in whose room a computer is installed and is primarily used by him or her is considered the **"primary user."** If a computer has multiple users, none of whom can be identified as the primary user, the Head of the Department should designate one person responsible for compliance with this policy.

### B. What Are End-User Computer Systems

Apart from the client PCs used by users, the University will consider servers **not directly administered by the Internet Unit** as end-user computers. If no primary user can be identified, the department must assume the responsibilities defined for end-users. Computer systems, if any, that act as servers providing services to other users on the Intranet/Internet—though registered with the Internet Unit are still considered under this policy as **"end-user computers."**

### C. Warranty and Annual Maintenance Contract

Computers purchased by any Section, Department, or Project should preferably have a **three-year on-site comprehensive warranty.** After the expiry of the warranty, computers should be covered under an **Annual Maintenance Contract (AMC).** Such maintenance should include operating-system reinstallation and checking for virus-related issues as well.

### D. Power Connection to Computers and Peripherals

All computers and peripherals should be connected to electrical points strictly through **UPS systems.** Power supply to the UPS should never be switched off, as continuous power is required for battery recharging.
Further, these UPS systems should be connected to electrical points that are properly earthed and have correctly laid electrical wiring.

### E. Network Cable Connection

While connecting a computer to the network, the network cable should be placed away from any electrical or electronic equipment, as such devices may interfere with network communication.

Further, no electrical or electronic equipment should share the same power supply as the computer and its peripherals.

**F. File and Print-Sharing Facilities**

File and print-sharing facilities on a computer over the network should be enabled **only when absolutely necessary.**
When files are shared through the network, they must be protected with passwords and provided with **read-only** access wherever possible.

**G. Shifting a Computer from One Location to Another**

A computer system may be moved from one location to another only with **prior written intimation** to the Internet Unit, since the Unit maintains a record of computer identification names and corresponding IP addresses.

Computer identification names follow a convention comprising the building name abbreviation and room number. Whenever any deviation from the list maintained by the Internet Unit is found for any computer system, its network connection will be disabled, and the user will be informed by email or phone (if identifiable). When the end-user meets the compliance requirements and informs the Internet Unit in writing or by email, the connection will be restored.

**H. Maintenance of Computer Systems Provided by the University**

For all computers purchased centrally by the University and distributed by the Estate Branch, the **University Computer Maintenance Cell (Computer Center)** will attend to complaints related to any maintenance problems.

**I. Non-Compliance**

MRDU faculty, staff, and students who do not comply with this computer hardware installation policy may expose themselves and others to network-related problems, which could result in damaged or lost files, inoperable computers, and loss of productivity. An individual's non-compliant computer can have significant adverse effects on other individuals, groups, departments, or even the entire University. Hence, it is critical to bring all computers into compliance as soon as they are identified as non-compliant.

**J. Internet Unit / Computer Center Interface**

If the Internet Unit finds a non-compliant computer affecting the network, it will notify the individual responsible for the system and request that it be brought into compliance. Such notification will be sent

via email or telephone, and a copy will be forwarded to the Computer Center, if applicable. The individual user must follow up on the notification to ensure that his or her computer achieves the necessary compliance.The Internet Unit will provide guidance as needed for the user to achieve compliance.

## 3.0 SOFTWARE INSTALLATION AND LICENSING POLICY

Any computer purchases made by individual departments or projects must ensure that such computer systems have all **licensed software** (operating system, antivirus software, and necessary application software) properly installed.

Respecting the **anti-piracy laws** of the country, the University IT Policy does **not** allow any pirated or unauthorized software installations on University-owned computers or on computers connected to the University's campus network. In case of any such instances, the University will hold the concerned department or individual **personally responsible** for any pirated software installed on computers located in their department or individual rooms.

### A. Operating System and Its Updating

1. Individual users should ensure that their respective computer systems have their operating systems updated with the latest service packs and patches through the Internet. This is particularly important for all **Microsoft Windows-based computers** (both PCs and servers). Updating the OS helps in fixing bugs and vulnerabilities detected periodically by Microsoft, for which it provides patches or service packs. Checking for updates and performing OS updates should be done at least **once a week.**
2. The University, as a policy, encourages the user community to adopt **open-source software** such as **Linux** and **OpenOffice** wherever possible.
3. Any Microsoft Windows-based computer connected to the network should access http://windowsupdate.microsoft.com for free updates. Such updating should be performed at least once a week. Even if systems are configured for automatic updates, it is the user's responsibility to ensure that the updates are being performed correctly.

### B. Antivirus Software and Its Updating

1. Computer systems used in the University must have **antivirus software** installed, and it must remain **active at all times.** The primary user of a computer system is responsible for ensuring compliance with this virus-protection policy.
2. Individual users must ensure that their respective computer systems have current antivirus software installed and maintained. They should verify that the software is functioning correctly. It should be noted that any antivirus software that is not updated or not renewed after its license period is practically useless. If these responsibilities exceed the end-user's technical skills, the user must seek assistance from a qualified service provider.

## C. Backups of Data

Individual users should perform **regular backups** of their important data. Virus infections often destroy data on an individual's computer, and without proper backups, recovery of lost files may be impossible.

Preferably, at the time of operating-system installation, the computer's hard disk should be partitioned into two volumes—typically **C** and **D.** The operating system and other software should be installed on the C drive, while user data files should be stored on the D drive.

In case of a virus problem, generally only the C volume becomes corrupted. In such cases, formatting only the C drive will minimize data loss. However, this is **not a foolproof solution.** Users should also keep copies of valuable data on removable storage devices such as **USB drives, external hard drives, or optical media (CD/DVD).**

## D. Non-Compliance

MRDU faculty, staff, and students who do not comply with this computer-security policy expose themselves and others to the risk of virus infections, which could result in:

- Damaged or lost files.
- Inoperable computers leading to loss of productivity.
- The risk of spreading infections to others.
- Confidential data being revealed to unauthorized persons.

An individual's non-compliant computer can have significant adverse effects on other individuals, groups, departments, or even the entire University. Hence, it is critical to bring all computers into compliance as soon as they are identified as non-compliant.

## E. Internet Unit / Computer Center Interface

If the **Internet Unit** finds a non-compliant computer, it will notify the individual responsible for the system and request that it be brought into compliance.

Such notification will be sent via **email or telephone**, and a copy will be forwarded to the **Computer Center**, if applicable. The individual user must follow up on the notification to ensure that his or her computer achieves the necessary compliance. The Internet Unit will provide guidance as needed for the individual to gain compliance.

## 4.0 NETWORK (INTRANET & INTERNET) USE POLICY

Network connectivity provided through the University—hereafter referred to as **"the Network"**—whether through an authenticated network-access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy.

The **Communication & Information Services (Internet Unit)** is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Any problems within the University's network should be reported to the Internet Unit.

### A. IP Address Allocation

Any computer (PC/Server) that will be connected to the University network must have an IP address assigned by the Internet Unit.

Following a systematic approach, a range of IP addresses is allocated to each building. Therefore, any computer connected to the network from that building will be assigned an IP address only from that address pool.

Further, each network port in the room from which a computer is connected will have internal binding with that IP address to prevent unauthorized use from any other location.

When a new computer is installed, the concerned user must download the application form for IP address allocation, complete it, and obtain the IP address from the Internet Unit.

An IP address allocated for a particular computer system must not be used on any other computer, even if the other computer belongs to the same individual and connects through the same port. IP addresses are assigned to **computers**, not to **ports.** Each computer must obtain its own IP address by submitting the prescribed requisition form.

### B. DHCP and Proxy Configuration by Individual Departments / Sections / Users

Using any computer at a user location as a **DHCP server** to connect multiple computers through a personal switch or hub and distribute IP addresses (public or private) is strictly prohibited. This practice is considered a direct violation of the University's IP Address Allocation Policy.

Similarly, configuration of proxy servers must be avoided, as it may interfere with services run by the Internet Unit. Even configuring any computer with an additional network interface card to connect another computer is considered a proxy or DHCP configuration.

Non-compliance with the IP Address Allocation Policy will result in disconnection of the port from which such a computer is connected to the network. The connection will be restored only after receiving written assurance of compliance from the concerned department or user.

## C. Running Network Services on the Servers

Individual departments or users connecting to the University network over the LAN may run server software (e.g., HTTP/Web server, SMTP server, FTP server) **only after** informing the Internet Unit **in writing** and meeting the requirements of the University IT Policy for running such services.

Non-compliance with this policy is a direct violation of the University IT Policy and will result in termination of their network connection. The Internet Unit takes no responsibility for the content of machines connected to the Network, regardless of whether those machines are University-owned or personal property.

The Internet Unit may disconnect client machines where potentially harmful software is detected or if the client's activity adversely affects network performance.

Access to remote networks using the University's network connection must comply with all the policies and rules of those networks. This applies to all networks connected to the University Network.

University network and computing resources are **not to be used for personal or commercial purposes.**

Network traffic will be monitored for **security** and **performance** reasons by the Internet Unit. Impersonation of an authorized user while connecting to the Network is a direct violation of this policy and will result in immediate termination of the connection.

## D. Dial-up / Broadband Connections

Computer systems that are part of the University's campus-wide network, whether University property or personal property must **not** be used for dial-up or broadband connections, as this violates University network security by bypassing firewalls and monitoring servers.

Non-compliance with this policy may result in withdrawal of the IP address allotted to the computer system.

## E. Wireless Local Area Networks

1. This policy applies, in its entirety, to all School, Department, or Division wireless local area networks (WLANs).
   In addition to the requirements of this policy, each School, Department, or Division must register every wireless access point with the Internet Unit, including the **Point of Contact** information.
2. Schools, Departments, or Divisions must inform the Internet Unit **before** using any radio spectrum for wireless LAN implementation.
3. Schools, Departments, or Divisions must **not** operate wireless LANs with unrestricted access. Network access must be restricted either through authentication or MAC/IP address filtering. Passwords and data must be encrypted.
4. If any School wishes to establish an **inter-building wireless network**, prior permission must be obtained from the University authorities through the Coordinator, Internet Unit.

## F. Internet Bandwidth Obtained by Other Departments

Internet bandwidth acquired by any Section or Department of the University under a research programme or project should ideally be **pooled** with the University's Internet bandwidth and treated as a **common institutional resource.**

Under exceptional circumstances that prevent such pooling, the concerned network must be **completely segregated** from the University's campus network.

All computer systems using that network must have a separate IP address scheme (private or public), and the University gateway should **not** be specified as an alternative gateway.

Such networks must be equipped with adequate network security measures as prescribed in the University IT Policy.

A copy of the **network diagram** containing the design details and IP address schemes must be submitted to the Internet Unit. Non-compliance with this policy will be treated as a **direct violation** of the University's IT Security Policy.

## 5.0 EMAIL ACCOUNT USE POLICY

In an effort to increase the efficient distribution of critical information to all faculty, staff, students, and University administrators, it is recommended to utilize the University's **email services** for formal University communication, academic correspondence, and other official purposes.

Email for formal communications will facilitate the delivery of messages and documents to the campus and extended communities or to specific user groups and individuals. Formal University communications are official notices from the University to faculty, staff, and students. These communications may include administrative content such as human-resources information, policy messages, general University notices, and official announcements.

To receive these notices, it is essential that the email account remains active and is used regularly. Staff and faculty may access their University email accounts by logging on to http://mail.mrec.ac.in with their user ID and password.

To obtain a University email account, users may contact the **Internet Unit** by submitting an application in the prescribed proforma to receive their account credentials and default password.

Users should be aware that by using the University's email facility, they agree to abide by the following policies:

1. The facility should be used primarily for **academic and official purposes**, and to a limited extent for personal use.
2. Using the facility for **illegal or commercial purposes** is a direct violation of the University's IT Policy and may lead to withdrawal of the facility. Illegal use includes, but is not limited to, unlicensed or illegal copying or distribution of software, sending unsolicited bulk email messages, and generating threatening, harassing, abusive, obscene, or fraudulent messages or images.
3. When sending large attachments, the user should ensure that the recipient has an email facility capable of receiving such large attachments.
4. Users should keep their mailbox usage within approximately **80% of the available quota**, as a "mailbox full" or "mailbox almost full" condition may cause incoming emails—especially those with large attachments—to bounce.
5. Users should not open any email or attachment from unknown or suspicious sources. Even if an email is from a known source but contains an attachment that seems suspicious or unusual, the user should confirm its authenticity with the sender before opening it. This is crucial for maintaining computer security, as such attachments may contain viruses capable of damaging valuable data.

6. Users should configure their email clients (e.g., Outlook Express, Thunderbird, etc.) on the computers they use regularly so that they can periodically **download emails** from the server to their local system, thereby freeing up space on the server.
   It is the user's responsibility to maintain backups of both incoming and outgoing mail.
7. Users should not share their email account credentials with others, as the **individual account holder is personally accountable** for any misuse of that email account.
8. Users should refrain from intercepting or attempting to access other users' email accounts, as this constitutes a violation of privacy.
9. When using shared computers, if an email account left open by another user is found, it must be **promptly closed** without viewing its contents by the person currently using the system.
10. Impersonating another user's email account will be treated as a **serious offence** under the University IT Security Policy.
11. It is ultimately each individual's responsibility to ensure that their email account remains in compliance with the University's email usage policy.
12. Any spam email received in the inbox should be forwarded to **admin@mrec.ac.in.**
13. Any legitimate email wrongly marked as spam should be forwarded to **systemadmin@mrec.ac.in.**
14. All emails detected as spam will appear in the **SPAM_MAIL** folder of the user's account.
    Users are advised to periodically check this folder for any important emails incorrectly flagged as spam.
    If such cases occur, the user should forward the sender's email ID to **systemadmin@mrec.ac.in** for corrective action.
    It is recommended to empty the SPAM_MAIL folder as frequently as possible.

## 6.0 WEBSITE HOSTING POLICY

### 1. Official Pages, Personal Pages and Affiliated Pages

**Official Pages:** Sections, departments, and Associations of Teachers / Employees / Students may have pages on MRDU's Intranet channel of the official website. Official web pages must conform to the University Web Site Creation Guidelines for website hosting. As of this date, the University's webmaster is responsible for maintaining the official website of the University: http://www.mrec.ac.in only.

**Personal Pages:** The University computer and network infrastructure is a limited resource owned by the University. It is recognized that each individual faculty member will have individual requirements for his or her pages. Hence, faculty may have personal pages linked to the official University website by sending a written request to the Internet Unit giving the URL of the page to be added. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not:

- violate any applicable export laws and regulations;
- constitute a copyright or trademark infringement;
- be used for commercial purposes;
- be used for political lobbying; or
- otherwise violate any local, state, or central government laws.

Personal pages must not host pages for other individuals or groups. Personal pages should explicitly state that the views expressed by the author are exclusively their own and not those of the University.

**Affiliated Pages:** Faculty may host web pages for "affiliated" professional organizations on department web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to the affiliated organization.

### 2. Web Pages for e-Learning

Though the University does not have this facility at present, this Policy addresses future requirements for web pages for e-learning authored as a result of the teaching/learning process.

Faculty may place class materials (syllabi, course materials, resource materials, etc.) on the web linked through the appropriate department pages.

Because the majority of student pages will be published on the University's web for e-learning, such pages must reflect the academic mission and must not be misrepresentative in any way or conflict with official

MRDU or other web sites. If a student publishes a fictional web site or a web site modeled after an existing institution or corporation, the site must be clearly identified as a class project.

The following are the storage and content requirements for class-generated student web pages:

**Servers:** It is recommended that pages be placed on the student information server, but pages developed for classes may also be placed on departmental servers or the main campus server meant for e-learning purposes.

**Maintenance:**

- If pages are published on the e-learning information server, they will be maintained under the default rules for personal e-learning pages.
- The instructor will maintain pages that are published on departmental servers or the main campus server meant for e-learning purposes.

**Content Disclaimer:** The home page of every class-generated site must include the MRDU Content Disclaimer (for pages published on the e-learning information server, the content disclaimer should be generated automatically).

**Class Information:** The home page of every class-generated site must contain the name of the class, the student's name(s), the date, and a link to the class home page.

**Pages Generated by Class Groups:** Pages produced by class groups, if placed on the e-learning information server, will be placed under the name of the designated group leader on the server.

**Official Pages:** If web pages developed for e-learning become part of the official MRDU page, they must be removed from the e-learning information server and departmental servers as class-generated pages (students may, of course, link to their work from personal student pages).

## 3. Student Web Pages

Though the University does not have this facility at present, this policy addresses future requirements for personal student web pages. Policies for student pages authored as a result of academic assignments are covered in Section 2 above. It is recognized that each individual student will have specific requirements for his or her pages. Because the University's computer and network infrastructure is a limited resource owned by the University, only student web pages related to assignments will be accepted for hosting on the student web server.

The contents of personal pages hosted by students, even on outside web sites, must not:

- violate any applicable export laws and regulations;
- constitute a copyright or trademark infringement;
- be used for commercial purposes;
- be used for political lobbying; or
- otherwise violate any local, state, or central government laws.

The following are the storage and content requirements for personal student web pages:

**Servers:** Pages will be placed on the student information server.

**Maintenance:** Pages published on the student information server will be maintained under the default rules for personal student pages.

**Content Disclaimer:** Every personal page will include the MRDU Content Disclaimer (the content disclaimer will be generated automatically).

## Responsibilities for Those Maintaining Web Pages

Sections, departments, units, and individuals are responsible for maintaining their own web pages.

MRDU web pages (including personal pages) must adhere to the MRDU Web Page Standards and Design Guidelines and should be approved by the **MRDU Web Pages Advisory Committee**.

## Policies for Maintaining Web Pages

Pages must relate to the University's mission. Authors of official MRDU and affiliated pages (not class-generated or personal) are required to announce their web presence by sending an announcement to **webmaster@mrec.ac.in**. Mails sent to this address will be placed in an MRDU Public E-Mail Folder on the University's official website. The announcement should include:

1. The URL.
2. A brief explanation of the content or purpose of the pages (e.g., administrative or academic unit, etc.). The primary page must include a link to the MRDU Home Page and, if applicable, contain additional links to the sponsoring organization or department.

## 7.0 UNIVERSITY DATABASE USE POLICY

### 1. Purpose

The purpose of this policy is to ensure the **secure, responsible, and ethical use of all databases** maintained by **Malla Reddy (MR) Deemed to be University (MRDU)** for academic, research, administrative, and operational functions.
This policy seeks to protect institutional data assets from unauthorized access, misuse, alteration, or loss and to promote compliance with statutory and regulatory requirements.

### 2. Scope

This policy applies to:

- All **faculty, staff, research scholars, students, and authorized users** of MRDU.
- All **servers, systems, and applications** that store, manage, or transmit institutional data, whether hosted **on-premises or on cloud platforms**.
- All categories of databases, including but not limited to:
    - Student Information System (SIS)
    - Human Resources Management System (HRMS)
    - Examination Management System
    - Research and Publications Repository
    - Learning Management System (LMS)
    - Finance and Accounts Database
    - Library Information Management System
    - Any other database approved by the University for institutional use

### 3. Policy Statement

The University maintains several databases that are critical to its functioning. These databases are **institutional property** and must be used **solely for authorized university purposes**.
All users must handle institutional data with **confidentiality, integrity, and accountability**, in accordance with this policy and applicable data-protection regulations.

### 4. User Responsibilities

All authorized users of University databases shall:

1. **Access Control:**

- Use only their **assigned credentials** to access databases.
- **Do not share passwords or access tokens** with others under any circumstances.
- Logout properly after completing work.

2. **Data Integrity:**
   - Enter, update, or modify data only when duly authorized.
   - Ensure that any data entered is **accurate, relevant, and complete**.
3. **Confidentiality:**
   - Maintain confidentiality of all institutional and personal data.
   - Avoid transferring database information to external sources without prior written approval from the competent authority.
4. **Legal and Ethical Use:**
   - Refrain from using University data for **commercial, political, or personal gain**.
   - Do not copy, download, or redistribute datasets without proper authorization.
5. **Reporting of Incidents:**
   - Immediately report any **data breach, suspected compromise, or unauthorized access** to the **INTERNET UNIT** or **University Computer Centre**.

## 5. Database Administration Responsibilities

The **Database Administrators (DBAs)** or designated staff under the **INTERNET UNIT** shall:

1. Maintain **secure configurations, user permissions, and role-based access controls**.
2. Schedule **regular database backups**, encryption, and restoration testing.
3. Apply timely **software patches and security updates**.
4. Monitor database activity logs to detect and prevent unauthorized use.
5. Ensure compliance with **Data Retention and Archival Policy** and **Information Security Guidelines**.
6. Provide access to data only upon written authorization from the **Registrar / Controller of Examinations / Director concerned**.

## 6. Data Classification

University data shall be classified into the following categories:

| Category | Description | Access Level |
|---|---|---|
| Confidential | Sensitive academic, financial, HR, and personal information | Restricted – Authorized Personnel Only |
| Internal | Routine institutional data for internal circulation | Staff and Faculty |
| Public | Approved data for public dissemination (e.g., results, circulars, reports) | Unrestricted |

## 7. Security and Compliance

- All database servers must be housed within secure network segments protected by the **University Firewall** and monitored by the **Network Operations Center (NOC)**.
- All institutional databases must comply with:
    - **UGC Guidelines for Data Protection and Information Security**
    - **Government of India IT Act, 2000 (as amended)**
    - **Data Privacy and Cybersecurity Guidelines of MRDU**
- Any violation of this policy may result in **suspension of access privileges**, **disciplinary action**, and/or **legal consequences**.

## 8. Data Retention and Disposal

- Data must be retained for the period specified in the **University Record Retention Policy**.
- Expired or obsolete data must be securely deleted using approved data-wiping procedures.
- Physical storage media used for backups must be stored in **restricted access areas** and periodically replaced.

## 8.0 RESPONSIBILITIES OF INTERNET UNIT

### A. Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained, and controlled by the **Internet Unit**.
2. The Internet Unit operates the campus network backbone to ensure that service levels meet the requirements of University sections, departments, and divisions served by the network, within the constraints of operational best practices.

### B. Physical Demarcation of Campus Buildings' Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of the Internet Unit.
2. Physical demarcation of newly constructed buildings to the backbone is also the responsibility of the Internet Unit. This includes determining the exact location at which the fiber-optic-based backbone terminates in the building. The Internet Unit also decides the type of connectivity (fiber-optic, wireless, or any other media) used to connect the building to the campus network backbone.
3. The Internet Unit will consult with the concerned clients to ensure that end-user requirements are met while protecting the integrity of the campus network backbone.
4. It is not the policy of the University to actively monitor Internet activity on the network; however, it may be necessary to examine such activity when a problem occurs or when optimizing traffic on the University's Internet links.

### C. Network Expansion

Major network expansion is also the responsibility of the Internet Unit. Every **3 to 5 years**, the Internet Unit reviews the existing networking facilities and assesses the need for possible expansion.Network expansion will be carried out by the Internet Unit when the University provides the necessary funds.

### D. Wireless Local Area Networks

1. Where access through Fiber Optic or UTP cables is not feasible, the Internet Unit may provide network connectivity through **wireless links**.
2. The Internet Unit is authorized to consider applications from sections, departments, or divisions for the use of radio spectrum prior to implementing wireless local area networks.
3. The Internet Unit is authorized to restrict network access for sections, departments, or divisions through wireless LANs using **authentication** or **MAC/IP address restrictions** as needed.

## E. Electronic Logs

Electronic logs generated through network-traffic monitoring shall be retained only as long as necessary for administrative purposes. Once their administrative need has ended, they must be securely destroyed.

## F. Global Naming and IP Addressing

The Internet Unit is responsible for maintaining a consistent system for the allocation of campus network services such as **IP addressing** and **domain name services**. It also monitors the network to ensure proper use of these services.

## G. Providing Net Access IDs and Email Accounts

The Internet Unit provides **Net Access IDs** and **email accounts** to individual users to enable them to use the campus-wide network and email facilities of the University. Accounts are issued upon receiving duly filled requests from individuals in the prescribed proforma.

## H. Network Operation Center

The Internet Unit operates a centralized **Network Operation Control Center (NOCC)**. The campus network and Internet facilities are available **24 hours a day, 7 days a week**. All network failures and cases of excessive utilization are reported to the Internet Unit's technical staff for problem resolution.

Routine **non-intrusive monitoring** of campus-wide network traffic is conducted by the Internet Unit. If traffic patterns suggest that system or network security, integrity, or performance has been compromised, the Internet Unit will analyze network traffic to identify the offending actions or equipment and apply protective restrictions until the issue is resolved. If necessary, a report will be sent to higher authorities in cases of serious violations.

## I. Network Policy and Technology Standards Implementation

The Internet Unit is authorized to take all reasonable steps necessary to ensure compliance with this and other network-related policies designed to protect the integrity and security of the campus network backbone.

## J. Receiving Complaints

The Internet Unit may receive complaints from the **Computer Center** if any network-related problems are observed while attending to end-user computer-system issues. Such complaints may be received via **email or telephone**.

The Internet Unit may also receive complaints directly from users who are unable to access the network due to network-related issues at their end. Such complaints are generally received via telephone.

The designated person in the Internet Unit will receive complaints from users or the Computer Center and coordinate with users, service engineers, or the internal technical team to resolve the problem within a reasonable time frame.

## K. Scope of Service

The Internet Unit is responsible solely for resolving network-related problems or providing services directly related to the University's network.

## L. Disconnect Authorization

The Internet Unit has the authority to disconnect any section, department, or division from the campus network backbone whose network traffic violates the practices set forth in this or any other network-related policy.

In situations where the normal flow of network traffic is severely degraded by a section, department, or division's machine or network, the Internet Unit will take corrective action in a manner that minimizes adverse effects on other network users.

If a section, department, or division is disconnected, the Internet Unit will provide the conditions that must be met for reconnection.

## 9.0 RESPONSIBILITIES OF UNIVERSITY COMPUTER CENTER

### A. Maintenance of Computer Hardware and Peripherals

The **Computer Center** is responsible for the maintenance of University-owned computer systems and peripherals that are either under **warranty** or **annual maintenance contract (AMC)** and whose responsibility has been officially entrusted to this Cell.

### B. Receiving Complaints

The **Computer Center** may receive complaints from the **Internet Unit** if any particular computer systems are causing network-related problems.

It may also receive complaints directly from users if any computer systems or peripherals under its maintenance have issues.

The designated person in the Computer Center receives complaints from users or the Internet Unit and coordinates with the service engineers of the respective computer brands to resolve the problem within a reasonable time frame.

### C. Scope of Service

The **Computer Center** is responsible only for resolving **hardware-related problems**, **operating system issues**, or problems related to **application software** that were **legally purchased by the University** and installed by the authorized company.

### D. Installation of Unauthorized Software

The **Computer Center** or its service engineers must not install or encourage the installation of any **unauthorized software** on users' computer systems. They must strictly refrain from obliging such requests.

### E. Reporting IT Policy Violation Incidents

If the **Computer Center** or its service engineers come across any applications or systems interfering with **network operations** or **violating the University's IT policies**, such incidents must be immediately reported to the **Internet Unit** and the **University authorities**.

## F. Reporting Incidents Related to Network Operations

When the network port of any computer system is disabled due to **virus activity** or any other issue affecting network performance, the **Internet Unit** will inform the **Computer Center**.

After taking the necessary corrective actions, the Computer Center or service engineers must inform the Internet Unit so that the port can be reactivated.

## G. Rebuilding the Computer System

When service engineers reformat a computer system and reinstall the operating system and other application software, care must be taken to assign the **same hostname, IP address, network mask, and gateway** as before.

After installing the OS, all patches and the latest service packs must also be installed. In the case of antivirus software, service engineers must ensure that the **latest engine and pattern files** are downloaded from the Internet.

Before reformatting the hard disk, a backup (dump) of **data files only** should be taken to restore them after reinstallation. Under no circumstances should **software files** from the infected hard disk dump be reused on the formatted disk.

## H. Coordination with Internet Unit

When there is uncertainty about whether a problem on a computer connected to the network is related to **network issues, software problems, or hardware malfunction**, the **Computer Center** or service engineers must coordinate with the **Internet Unit staff** to resolve the issue through joint effort.

This task should **not** be left to the individual user.

## 10.0 RESPONSIBILITIES OF DEPARTMENTS OR SECTIONS

### A. User Account

Any Centre, Department, Section, or other entity can connect to the University network using a legitimate **User Account (Net Access ID)** for the purpose of verifying its affiliation with the University. The user account will be provided by the **Internet Unit** upon submission of the prescribed application form.

Once a user account is allocated for accessing the University's computer systems, network, mail, web services, and other technological facilities, the account holder becomes personally responsible and accountable to the University for all actions performed using that account.

Users must take reasonable precautions to prevent unauthorized access to their accounts. These include:

- Using complex passwords.
- Not sharing passwords with others.
- Avoiding writing passwords in accessible places.
- Changing passwords regularly.
- Maintaining separate passwords for Net Access ID and email account ID.

As members of the MRDU community, users are expected to respect the University's reputation in all electronic communications, both within and outside the University.

It is the user's responsibility to understand and follow the **University IT Policy** to ensure the proper use of the University's technology and information resources.

### B. Logical Demarcation of Department/Section/Division Networks

In some cases, a Section, Department, or Division may have created an internal network within its premises.
In such cases, the respective Section, Department, or Division assumes full responsibility for the network services provided on its internal network, including operations on its side of the University network backbone.

Each Section, Department, or Division must ensure that its network operations do not negatively affect other network segments connected to the University's backbone.

Each Section, Department, or Division should identify at least one **Point of Contact (POC)** and communicate the details to both the **Internet Unit** and the **Computer Center**, enabling direct communication in case of network or system-related issues.

## C. Supply of Information by Sections, Departments, or Divisions for Publishing/Updating the MRDU Website

All Schools, Centres, Departments, or Divisions must provide updated information about their activities periodically (at least once a month or earlier).

A **hard copy** of such information, duly signed by the competent authority, and a **soft copy** must be submitted to the webmaster in the **Internet Unit**. This policy also applies to advertisements, tender notifications published in newspapers, and events organized by the Section, Department, or Division.

Links to any new web pages created for specific purposes or events may be added to the official University website upon receiving a written request. If such web pages are to be incorporated directly into the University's official website, the content (including text and images, if any) must conform to the existing web design and format.

Requests, along with the soft copy of content, must be forwarded to the **Director, Internet Unit** well in advance.

## D. Setting Up of Wireless Local Area Networks / Broadband Connectivity

1. This policy applies to all Schools, Departments, or Divisions setting up wireless local area networks or broadband connections within the academic complex. Each unit must register its **wireless access points** with the **Internet Unit**, including POC information.
2. Obtaining broadband connections and using computers alternately on the broadband and the University's campus-wide network is a **direct violation** of the University IT Policy. Broadband connections are not permitted within the academic complex.
3. Schools, Departments, or Divisions must obtain permission from the **Internet Unit** before implementing any wireless local area network.
4. Wireless networks must not have unrestricted access. Network access must be restricted through authentication or MAC/IP address filters, and passwords and data must be encrypted.
5. Inter-building wireless networks are governed by the University IT Policy; therefore, Schools/Centres must not set up such networks without prior information to the **Internet Unit**.

## E. Security

By connecting to the University network backbone, each School, Department, or Division agrees to abide by the **Network Usage Policy** under the **University IT Security Policy**.

Any network security incidents will be resolved in coordination with the designated Point of Contact (POC) in the originating department. If no POC is available, the affected computer will be disconnected from the network until compliance is achieved.

## F. Preservation of Network Equipment and Accessories

All routers, switches, fiber optic cabling, UTP cabling, network inlets, racks, UPS systems, and batteries installed across the campus are **property of the University** and are maintained by the **Internet Unit**.

Tampering with these components by departments or individual users constitutes a **violation of the IT Policy**.
Tampering includes, but is not limited to:

- Removal of network inlet boxes.
- Removal or relocation of UTP cables.
- Opening racks or altering port connections at jack-panel or switch levels.
- Removing UPS units or batteries from switch rooms.
- Disturbing the existing network infrastructure during renovations.

The Internet Unit will not be responsible for rectifying such tampering, and network connectivity to the affected segment or user will remain disconnected until compliance is restored.

## G. Additions to the Existing Network

Any addition to the existing network by a Section, Department, or individual must strictly follow the **University Network Policy**, obtain prior permission from the competent authority, and inform the **Internet Unit**.

For any network expansion, the following procedures must be followed:

- All internal network cabling must conform to **CAT6 UTP standards**.
- UTP cabling must adhere to **structured cabling standards**—no loose or hanging cables are permitted.
- UTP cables must be properly terminated at both ends.

- Only **managed switches** should be used. Such switches must have web-enabled management modules. The use of unmanaged switches is **prohibited** under University IT Policy.

Managed switches allow monitoring through web interfaces, enabling the Internet Unit to assess their health remotely. However, **hardware maintenance** of any such expanded network segment will remain the sole responsibility of the department or individual.

If any network problem arises due to an offending computer behind an unmanaged hub/switch, and the offending system cannot be located, the **network connection to that hub/switch will be disconnected** until compliance is met.

Since managed switches require IP addresses, departments may obtain them from the Internet Unit upon request.

## H. Structured Cabling in New Buildings

All new buildings constructed within the academic complex must include **structured cabling** as part of their building plans, similar to electrical and telephone wiring.
The Engineering Branch should make provisions for at least one network point per room, and all network cabling must strictly adhere to the structured cabling standards for Local Area Networks (LAN).

## I. Campus Network Services Use Agreement

The **"Campus Network Services Use Agreement"** must be read by all University members seeking access to the campus network. This document is available on the University intranet.

All provisions of this policy form part of the agreement.
Any Section, Department, Division, or individual using the campus network facility is deemed to have accepted the **University IT Policy**. Users are responsible for being aware of this policy. Ignorance of its existence is **not an acceptable excuse** for any violation.

## J. Enforcement

The **Internet Unit** periodically scans the University network to ensure compliance with the **Network Use Policy**.
Failure to comply may result in the **discontinuation of service** for individuals responsible for policy violations.

## 11.0 RESPONSIBILITIES OF ADMINISTRATIVE UNITS

The **Internet Unit** requires the latest information from various Administrative Units of the University to:

- Provide network and other IT facilities to new members of the University.
- Withdraw these facilities from members leaving the University.
- Keep the MRDU website up to date in terms of content and information.

The information required from Administrative Units includes:

- Details about new appointments or promotions.
- Details about superannuations or termination of services.
- Information on new student enrolments.
- Details on expiry of studentship or removal of names from the rolls.
- Notification of any action by University authorities that makes an individual ineligible to use University network facilities.
- Information on important events, developments, or achievements.
- Information regarding rules, procedures, and facilities.

Information related to items **A–E** should reach the **Director (Internet Unit)**, while information related to items **F and G** should reach the **Webmaster** well in time.

A **hard copy** of the information, duly signed by the competent authority, along with a **soft copy** (through mobile storage devices or via email), must be sent to the **Internet Unit** to reach the designated officers promptly.

## 12.0 GUIDELINES ON COMPUTER NAMING CONVENTIONS

1. To troubleshoot network problems and provide timely service, it is essential to quickly identify computers connected to the campus network. All computer names on the campus network must follow the University's standard naming conventions. Computers not following these conventions may be removed from the network at the discretion of the Internet Unit.
2. All computers should adhere to the prescribed naming format defined by the University IT Policy.

## 13.0 GUIDELINES FOR RUNNING APPLICATION OR INFORMATION SERVERS

### A. Permission to Run Servers

1. Sections or Departments may run an application or information server with proper authorization.
2. Individual faculty, staff, or students on the MRDU campus may not run personal, publicly available servers (such as FTP, chat, news, games, mail, or ISP servers) on the MRDU network.

### B. Responsibilities of Sections/Departments Running Servers

Sections or Departments operating an application or information server must ensure the following:

1. The content and services hosted comply with the MRDU Guidelines for Web Presence.
2. Obtain a dedicated IP address from the Internet Unit for the server.
3. Register the server's hostname in the DNS server for IP address resolution. The University's naming convention must be followed.
4. Enable only those services that are essential for the functioning of the server.
5. Protect the server from virus attacks and intrusions by installing and maintaining security software such as antivirus, intrusion prevention systems, personal firewalls, and anti-spam tools.
6. Periodically update the operating system and all security software.
7. Provide written information to the Internet Unit before installing such servers and obtain the necessary IP address.

Sections or Departments must provide their own hardware, software, and support staff to maintain these servers. For general guidance on whether to host a departmental or organizational web server, contact the Internet Unit.

## 14. GUIDELINES FOR HOSTING WEB PAGES ON THE INTERNET/INTRANET

### Mandatory Requirements

1. Provide the full Internet email address of the web page maintainer.
2. Include a link to the MRDU Home Page from the department's home page.
3. Include a "Return to Department's Home Page" link on all subpages.
4. Keep all pages up to date—proofread content and test links before publishing, and perform regular checks to maintain working links.
5. Understand and use HTML tags appropriately.
6. Provide printer-friendly versions of important web pages.

### Recommended Practices

1. Display update timelines (e.g., "Last updated: March 2025").
2. Include a "What's New" section for new content.
3. Add a caution statement if a link leads to large files or images.
4. Indicate restricted access where applicable.
5. Avoid browser-specific features or terminology.
6. Use clear link text instead of phrases like "Click here."
7. Maintain visual consistency across all related pages.
8. Add a copyright statement where appropriate.
9. Keep home pages concise and simple.
10. Avoid using large or multiple graphics on a single page.
11. Provide navigational aids such as "Home," "Table of Contents," and "Next Page."
12. Maintain working links to all referenced pages.
13. Design web pages to be easy to maintain for current and future maintainers.
14. Avoid linking to unfinished or test pages; place drafts in "test," "temp," or "old" directories.
15. Test web pages across different browsers, monitors, and connection types (LAN and modem).
16. Test pages with primary user groups—a mix of high-speed and low-speed users.
17. Conform to standard HTML coding practices.

## 15. GUIDELINES FOR DESKTOP USERS

These guidelines apply to all members of the **MRDU Network User Community** and are intended to strengthen **desktop security** due to increasing hacker activity.

### Recommended Practices

1. All desktop computers must have the latest version of antivirus software (e.g., Symantec or Quick Heal) configured for regular automatic updates from the central server.
2. Ensure all operating system updates and patches are applied during installation and regularly thereafter (recommended frequency: once a week).
3. Each desktop must have an administrator account separate from the regular login account, and its password should be changed from the default.
4. Passwords must be:
    - 6–8 characters long.
    - Include punctuation such as !$%&*,.?+-=.
    - Begin and end with letters.
    - Not contain `#@"'`` characters.
    - Be unique (not reused).
    - Avoid using personal or departmental names, room numbers, or other identifiable terms.
    - Changed periodically, especially if compromise is suspected.
    - Never left blank or set as "NOPASS."
    - Always replaced from default software installation passwords.
5. User login passwords must follow the same rules as above.
6. Disable the Guest Account on all systems.
7. Enable built-in firewalls on Windows XP or later systems.
8. Use a personal firewall (usually bundled with antivirus software) if the operating system lacks one.
9. If a computer becomes compromised, reinstall all software from original media after formatting the hard drive. Copy only data files, ensuring no virus transfer from old disks.
10. Do not install Microsoft IIS or activate any of its functions unless absolutely necessary.
11. Start from a secure configuration (no shares, no guest access) and open services only as needed.
12. Implement a regular data backup strategy (daily or weekly) to minimize damage from data loss.
13. If a computer is compromised, the Internet Unit will disable its network port until the issue is resolved per these guidelines.
14. Departments with their own subnets may request the Internet Unit to apply standard filters or scan departmental servers for vulnerabilities upon request.

# 16.VIDEO SURVEILLANCE POLICY

The system comprises fixed-position cameras; pan–tilt–zoom (PTZ) cameras; monitors; multiplexers; digital recorders; SAN/NAS storage; and public information signs.

Cameras will be located at strategic points on the campus, principally at the entrance and exit points of sites and buildings. No camera will be hidden from view, and none will be positioned to focus on the frontages or rear areas of private accommodation.

Signs will be prominently placed at strategic points and at the entrance and exit points of the campus to inform staff, students, visitors, and members of the public that a CCTV/IP camera installation is in use.

Although every effort has been made to ensure maximum effectiveness of the system, it is not possible to guarantee that the system will detect every incident occurring within the area of coverage.

## Purpose of the System

The system has been installed by the University with the primary purposes of reducing the threat of crime generally, protecting University premises, and helping to ensure the safety of all staff, students, and visitors, consistent with respect for individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those with criminal intent.
- Assist in the prevention and detection of crime.
- Facilitate the identification, apprehension, and prosecution of offenders in relation to crime and public order.
- Facilitate the identification of any activities or events which might warrant disciplinary proceedings against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be, taken.
- For security staff, provide management information relating to employee compliance with contracts of employment.

## The System Will Not Be Used

- To provide recorded images for the world wide web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking.

## Covert Recording

Covert cameras may be used only under the following circumstances, with the written authorization or request of a senior officer (Registrar) and where the use has been assessed by the Head of Security and Facilities Services and the Data Protection Officer:

- Informing the individual(s) concerned that recording is taking place would seriously prejudice the objective of making the recording; and
- There is reasonable cause to suspect that unauthorized or illegal activity is taking place or is about to take place.

Any such covert processing will be carried out only for a limited and reasonable period consistent with the objectives of the recording and will relate only to the specific suspected unauthorized activity. The decision to adopt covert recording will be fully documented and will set out how the decision was reached and by whom.

# 17.THE SECURITY CONTROL ROOM

Images captured by the system will be monitored and recorded in the **Security Control Room** ("the Control Room"), twenty-four hours a day throughout the year. Monitors are not visible from outside the Control Room.

No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to duty controllers, authorized members of senior management, police officers, and any other person with statutory powers of entry.

Staff, students, and visitors may be granted access to the Control Room on a case-by-case basis and only with written authorization from the Registrar. In an emergency, and where it is not reasonably practicable to obtain prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room.

Before allowing access, staff will verify the identity of any visitor and confirm that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization, the person who granted authorization, and the times of entry to and exit from the Centre. A similar log will be kept of staff on duty in the Security Control Room and any visitors granted emergency access.

## Security Control Room Administration and Procedures

Details of administrative procedures relating to the Control Room will be set out in a **Procedures Manual**, a copy of which is available for inspection by prior arrangement, subject to stated reasons for the request.

Images of identifiable living individuals are subject to the provisions of the prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day-to-day compliance with the Act.

All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

## Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP camera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the operational and administrative functions arising from the use of CCTV/IP cameras.

## Recording

Digital recordings are made using digital video recorders operating in time-lapse mode. Incidents may be recorded in real time.

Images will normally be retained for fifteen days from the date of recording and then automatically overwritten, and the log updated accordingly. Once a hard drive has reached the end of its use, it will be erased prior to disposal and the log will be updated.

All hard drives and recorders shall remain the property of the University until disposal or destruction.

## Access to Images

All access to images will be recorded in the **Access Log** as specified in the Procedures Manual.

Access to images will be restricted to staff who need access in accordance with the purposes of the system.

## Access to Images by Third Parties

Disclosure of recorded material will be made to third parties only in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism or disorder.
- Prosecution agencies.
- Relevant legal representatives.
- The media, where the assistance of the general public is required in identifying a victim or a perpetrator of a crime.
- People whose images have been recorded and retained, unless disclosure to the individual would prejudice criminal enquiries or proceedings.
- Emergency services in connection with the investigation of an accident.

## Access to Images by a Subject

CCTV/IP camera digital images that identify a person are personal data and are covered by the Data Protection Act. Anyone who believes they have been filmed by CCTV/IP camera is entitled to request a copy of the data, subject to exemptions contained in the Act. They do not have a right to instant access.

A person whose image has been recorded and retained and who wishes to access the data must apply in writing to the **Data Protection Officer**. Subject Access Request Forms are obtainable from the Security Office between 10:20 and 14:00 and 14:30 and 18:00 Monday to Saturday (except the second and fourth Saturday), except when the University is officially closed, or from the Data Protection Officer/Records Office during the same hours.

The Data Protection Officer will arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, nor request a copy from anyone else. All communications must go through the University Data Protection Officer. A response will be provided promptly and, in any event, within forty days of receiving the required fee and information.

The Data Protection Officer has the right to refuse a request for a copy of the data, particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. All such requests will be referred to the Security Control Room Supervisor by the Data Protection Officer.

If it is decided that a data-subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

## Request to Prevent Processing

An individual has the right to request prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that individual or another person.

All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Data Protection Officer, who will provide a written response within 21 days of receiving the request, setting out their decision. A copy of the request and response will be retained.

## 18.COMPLAINTS

It is recognized that members of the University and others may have concerns or complaints about the system's operation. Any complaint should be addressed in the first instance to the Security Control Room Supervisor. If, after following the steps set out, the complaint remains unresolved, the complainant may invoke the University Centralized Complaints Procedure by obtaining and completing a University Complaints Form. Complaints forms may be obtained from the Security Office and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer. These rights do not alter existing rights of members of the University or others under any relevant grievance or disciplinary procedures.

## 19.COMPLIANCE MONITORING

The contact point for members of the University or members of the public wishing to enquire about the system will be the Security Office, which will be available during the hours of **10:20–14:00** and **14:30–18:00**, Monday to Saturday (except the second and fourth Saturday), except when the University is officially closed.

## 20.POLICY REVIEW AND CONTINUOUS IMPROVEMENT

The **Information Technology (IT) Policy** of **MRDU** shall be treated as a *living document* subject to periodic review, modification, and continuous improvement to ensure its ongoing relevance, effectiveness, and alignment with emerging technologies, regulatory frameworks, and institutional goals.

### 1. Policy Review Process

- The INTERNET UNIT, in coordination with the University Computer Centre, IQAC, and IT Policy Committee, shall periodically review the IT Policy at least once in every three years, or earlier if required due to technological or statutory changes.
- The review shall include evaluation of:
    - The adequacy of existing provisions in addressing evolving IT and cybersecurity needs.
    - Compliance with UGC, AICTE, Data Protection, and Government of India (GoI) guidelines.
    - The effectiveness of implementation, user awareness, and security performance.

## 2. Continuous Improvement

- Feedback shall be collected from:
  - Academic and administrative users.
  - System administrators and network managers.
  - IQAC audit findings, internal audits, and external accreditation bodies.
- All approved revisions will be incorporated through the **Document Revision Process** and will be communicated university-wide through circulars, intranet updates, and official email notifications.

## 3. Approval and Version Control

- Each revision of this policy shall be approved by the Director – IQAC, endorsed by the Registrar, and ratified by the Vice-Chancellor before issue.
- The Document Control Sheet and Revision History sections below record all approved modifications to maintain transparency and traceability.

## MALLA REDDY (MR) DEEMED TO BE UNIVERSITY

### DOCUMENT CONTROL SHEET

| Document Title | Information Technology (IT) Policy |
|---|---|
| **Document Code** | MRDU/IQAC/ITP/2025 |
| **Version No.** | 1.0 |
| **Prepared By** | INTERNET UNIT & UNIVERSITY COMPUTER CENTRE |
| **Reviewed By** | Vice Chancellor, Pro VC & Registrar |
| **Approved By** | EC |
| **Effective Date** | 12 January 2026 |
| **Next Review Date** | 12 January 2029 |
| **Distribution** | All Academic & Administrative Departments, INTERNET UNIT, Computer Centre, IQAC Portal |
| **Confidentiality Level** | Internal – Restricted Circulation |
| **File Location** | MRDU Intranet Channel → Policy Repository → IT Policy Folder |

### DOCUMENT REVISION HISTORY

| Version No. | Date of Revision | Section / Clause Revised | Nature of Revision / Description | Prepared / Updated By | Approved By |
|---|---|---|---|---|---|
| 1.0 | 01 July 2025 | - | Initial Release of MRDU IT Policy | INTERNET UNIT / IQAC | EC |

## Appendix – I

## MALLA REDDY (MR) DEEMED TO BE UNIVERSITY

**SECUNDERABAD – 500 100**

**INTERNET UNIT**

## APPLICATION FOR IP ADDRESS ALLOCATION

**Note:** All fields are mandatory. Please fill in all details clearly and accurately.

**1. Location of the System**
Section / Department: _____
Room No.: _____ Floor / Lab No.: _____
Occupied by: _____

**2. Identification Name of the System (Hostname):**

**3. I/O Box Number:** _____

**4. Make of the System:**
☐ ACER ☐ COMPAQ ☐ HCL ☐ IBM ☐ HP ☐ DELL ☐ Other (Specify): _____

**5. MAC / Physical / Adapter Address:**

**6. Operating System:**
☐ Windows 95 ☐ Windows 98 ☐ Windows 2000 ☐ Windows XP ☐ Linux ☐ Solaris ☐ Other (Specify): _____

**7. Network-Based Applications Running on the System:**
☐ Yahoo Messenger ☐ MSN Messenger ☐ AOL ☐ Microsoft Anti-Spyware ☐ SPSS
☐ Others (Specify): _____

**8. Network Connection Type:**
☐ Directly connected to LAN
☐ Connected through Hub/Switch located in the same room
☐ Connected through Hub/Switch located in a different room

**9. If the System Is Configured as a Server, Specify the Services Enabled:**
☐ HTTP ☐ SMTP ☐ FTP ☐ Sendmail ☐ NFS ☐ POP3 ☐ IMAP ☐ SMB ☐ MySQL ☐ TELNET ☐ Any Other (Specify): _____

**10. System Usage Type:**
☐ Single User ☐ Multiple Users

**11. Antivirus Software Installed:**

**Date: _____** **Signature of the Applicant: _____**

---

## For Office Use Only (Internet Unit)

| Particulars | Details / Remarks |
|---|---|
| IP Address Allocated | |
| Subnet Mask | |
| Gateway | |
| VLAN / Switch Port | |
| Verified By | |
| Authorized By | |
| Date of Allocation | |

## Appendix – II

## MALLA REDDY (MR) DEEMED TO BE UNIVERSITY

### SECUNDERABAD – 500 100

## REQUISITION FORM FOR FACULTY E-MAIL ACCOUNT

**1. Full Name:** _____

**2. Designation:** _____

**3. Department:** _____

**4. Mobile Number:** _____

**5. Preferred E-mail Account Name:**

Option 1: _____ @mrec.ac.in

Option 2: _____ @mrec.ac.in

---

**Date:** _____ **Signature of the Applicant:** _____

**Head of the Department:** _____

---

### User Counterfoil

The following official e-mail ID has been created for
**Prof./Dr./Mr./Ms.** _____

on _____ @mrdu.edu.in

---

**Signature on behalf of Coordinator, INTERNET UNIT**

## Appendix III

**MALLA REDDY (MR) Deemed to be University**

**SECUNDERABAD-500100**

## REQUISITION FORM FOR STUDENTS'E-MAIL ACCOUNT

**(USEBLOCKLETTERSONLY)**

1. Full Name:_____
2. Programme:_____
3. University:_____
4. Department:_____
5. Year of Admission:_____
6. Semester: I/II
7. Permanent Address:

_____
_____

8. Local Address:

_____
_____

9. Telephone/Mobile No.if any:_____
10. Identity Card No.:_____

**Declaration**

The above information furnished by me is correct, and I undertake to abide by the rules and regulations of the University for proper use of email facility for my research work purpose.

Date: **SIGNATUREOFTHESTUDENT**

_____ _____
_____

Application for email account recommended by

Signature & Stamp of **HOD Counterfoil**

**Mr./Ms.**_____

***Email Account:**_____**@mrdu.edu.in**

Signature on behalf of Co-ordinator