MALLA REDDY VISHWAVIDYAPEETH
(DEEMED TO BE UNIVERSITY)

Recognised Under Section 3 of The UGC Act, 1956, Vide Notification No.9-4/2024-U.3(A) by Department of Higher Education, Ministry of Education, Government of India.

Ref. No: MRV/Policies/022 **Date: 05.10.2026**

NOTIFICATION

In pursuance of the resolution passed by the Executive Council at its meeting held on 03/10/2026 **vide Resolution No. EC-08-07 as adopted on 3rd October 2026.**

It is hereby notified for the information of all concerned that **Malla Reddy Vishwavidyapeeth**, has published the **"Information Technology and Data Security Policy"** for information to all concerned. The **Information Technology and Data Security Policy Document** mainly comprises the following parts:

- **Hardware & Software Licensing**
- **Network & Email Use**
- **Web Hosting & Database Use**
- **Role of Users**

The **Information Technology and Data Security Policy Document** will serve as detailed guidelines and will be useful to all concerned. It will come into force with immediate effect.

MALLA REDDY VISHWAVIDYAPEETH ★ Suraram Hyderabad ★ (Deemed to be University)

Registrar

Copy to

1. Hon'ble Chancellor, Malla Reddy Vishwavidyapeeth
2. Hon'ble Vice Chancellor, Malla Reddy Vishwavidyapeeth
3. Pro Vice Chancellor, Academics & Accreditation, Malla Reddy Vishwavidyapeeth
4. Pro Vice Chancellor, MRTC, Malla Reddy Vishwavidyapeeth
5. Deans/ Principals/ Directors/ of all Constituent Colleges/Schools of Eminence, Malla Reddy Vishwavidyapeeth
6. Director (Research), Malla Reddy Vishwavidyapeeth
7. Controller of Examinations, Malla Reddy Vishwavidyapeeth
8. Finance Officer, Malla Reddy Vishwavidyapeeth
9. IQAC Coordinator, Malla Reddy Vishwavidyapeeth
10. Web master for uploading on the Malla Reddy Vishwavidyapeeth Website.



MALLA REDDY VISHWAVIDYAPEETH

(Deemed to be University)

Recognised under section 3 of The UGC Act, 1956, vide Notification No.9-4/2024-U.3(A) by Department of Higher Education, Ministry of Education, Government of India.

MRV INFORMATION TECHNOLOGY AND DATA SECURITY POLICY

INFORMATION TECHNOLOGY AND DATA SECURITY POLICY

1. Purpose and Applicability

This policy governs the acceptable use, security, and management of all Information Technology (IT) resources hardware, software, networks, data, and digital services owned, leased, or operated by Malla Reddy Vishwavidyapeeth. It applies to all students, faculty, staff, contractors, and visitors who access MRV's IT resources across all constituent colleges and Schools of Eminence, and is issued in compliance with the Information Technology Act, 2000, CERT-In Directions, the Digital Personal Data Protection Act, 2023, and applicable UGC guidelines.

Key Definitions

- **IT Resources:** all computing hardware, software, network infrastructure, data, cloud services, and digital accounts provided or authorized by MRV.
- **User:** any student, faculty, staff member, contractor, or authorized third party accessing MRV's IT Resources.
- **Cyber Incident:** any event that compromises the confidentiality, integrity, or availability of an IT Resource, including malware, unauthorized access, denial-of-service, or data breach.
- **Personal Data:** any data about an identifiable individual, as defined under the Digital Personal Data Protection Act, 2023.
- **Data Fiduciary / Data Principal:** MRV, as the entity determining the purpose of processing personal data (Data Fiduciary), and the individual to whom the data relates (Data Principal), as defined under the DPDP Act, 2023.



2. IT Governance Structure

Role	Key Responsibilities
IT Governance / Security Committee	Approves this policy, IT strategy, and security roadmap; reviews major incidents; chaired by a senior officer designated by the Vice-Chancellor
Chief Information Security Officer (CISO) / IT Head	Owns day-to-day implementation, risk assessment, vendor security review, and CERT-In/DPDP Board incident reporting
University Computer Centre / IT Services	Network operations, server/hosting administration, account provisioning, backups, patching, helpdesk
Constituent / Schools of Eminence	Nominate a college IT coordinator; ensure local compliance, asset inventory, and timely incident reporting
All Users (staff, faculty, students)	Comply with this policy, protect credentials, report incidents promptly, complete mandatory security-awareness training

3. Acceptable Use of IT Resources

3.1 Hardware and End-User Systems

- University-provided computers and peripherals are for official academic/administrative use; the primary user is responsible for its safe custody and appropriate use.
- Relocation, addition, or modification of hardware/network points requires prior intimation to IT Services; unauthorized rewiring or tapping of network points is prohibited.
- All systems must run a licensed, updated operating system with current security patches; use of open-source/licensed software is encouraged to control cost and licensing risk.
- Installation of unauthorized or pirated software is prohibited; only software approved by IT Services may be installed on University systems.



3.2 Software Asset and License Management

- IT Services shall maintain a central inventory of licensed software and hardware assets, including purchase date, warranty/AMC status, and assigned custodian.
- Only software procured and approved through the University's official channel may be deployed on institutional systems; use of unlicensed or cracked software exposes both the user and the University to legal liability and is strictly prohibited.
- Hardware nearing end-of-warranty or end-of-life shall be flagged for renewal, replacement, or secure decommissioning (including data wiping) by IT Services.

3.3 General Conduct

- IT resources shall be used primarily for academic, research, and official purposes; commercial, illegal, or personal-business use is prohibited.
- Users shall not attempt to bypass security controls, access another user's account, or interfere with network operations.
- Use of IT resources to harass, defame, or transmit offensive, obscene, or unlawful content is strictly prohibited and will be treated as misconduct under MRV's Disciplinary Policy.

4. Account, Access, and Password Management

- Every user is issued a unique login ID; sharing of credentials with any other person is strictly prohibited and treated as a security violation.
- Passwords must be a minimum of 8 characters with a mix of upper/lower case, numerals, and special characters, and changed at least every 90 days.
- Multi-Factor Authentication (MFA) is mandatory for email, ERP, financial systems, and any remote access to University systems.
- Access to systems and data is granted on a role-based, least-privilege basis; access rights are reviewed periodically and revoked immediately on change of role or separation from the University.
- Administrative/privileged accounts are limited to authorized IT personnel and subject to enhanced logging and periodic audit.



5. Network, Wi-Fi, and Internet Use

- IP address allocation, DHCP, and proxy configuration are managed centrally by IT Services; departments/individuals may not independently configure these services.
- Running unauthorized network services (DHCP, proxy, mail, or file-sharing servers) on the campus network is prohibited without written IT Services approval.
- Departments requiring wireless access points must obtain prior clearance from IT Services; unauthorized personal Wi-Fi routers/hotspots on the campus network are prohibited.
- Internet bandwidth is a shared resource; excessive or non-academic consumption (streaming, large downloads, torrents) may be throttled or restricted, especially during peak academic hours.
- MRV does not routinely monitor content but reserves the right to inspect network traffic and logs in connection with a security incident, legal requirement, or policy violation investigation.

6. Email and Digital Communication

- Official University email accounts must be used for all academic and administrative correspondence; auto-forwarding of official email to personal accounts is discouraged.
- Users must not open attachments or links from unknown or suspicious senders, and must report suspected phishing emails to IT Services immediately.
- Mailbox storage should be kept within the allotted quota; large attachments should be shared via approved institutional file-sharing tools rather than email where possible.
- Impersonation of another person's email identity, or unauthorized interception of another user's communication, is a serious violation attracting disciplinary and, where applicable, legal action.

7. Website, Server, and Application Hosting

- All official MRV web pages and digital content are managed and approved by the University's designated web/IT authority; unauthorized publication under the University's domain is prohibited.



- Departments and Schools seeking to host applications, information servers, or e-learning pages must register the service with IT Services and comply with the University's security-hardening baseline.
- All externally facing servers/applications must undergo a security review before go-live, and periodic vulnerability assessment thereafter.
- Content published on official pages must carry a disclaimer where relevant, and must not include personal, defamatory, or unauthorized material.

8. Data Protection and Privacy

MRV is committed to protecting personal data processed in the course of its academic and administrative functions, in compliance with the Digital Personal Data Protection Act, 2023.

- Personal data (of students, staff, alumni, and applicants) shall be collected only for a lawful, specified purpose, with consent or another lawful basis under the DPDP Act, and used only for that purpose.
- Data shall be classified and access-controlled as summarised below; Confidential/Restricted data must be encrypted at rest and in transit:

Classification	Examples	Handling Requirement
Public	Prospectus, published research, marketing content, public website pages	May be freely shared; standard integrity controls apply
Internal	Internal circulars, meeting minutes, non-sensitive operational data	Accessible to MRV staff/faculty only; not for external distribution without approval
Confidential	Student academic records, staff personal data, financial records, unpublished research	Access restricted to authorized roles; encryption at rest/in transit; audit logging required
Restricted	Examination question papers, medical/health records, ICC/POSH case files, payment card data	Highest level of control; encryption mandatory; access strictly need-to-know and logged; breach triggers incident-response and DPDP reporting

VISHWAVIDYAPEETH Suraram Hyderabad (Deemed to be University)

- Data shall be retained only as long as necessary for the purpose for which it was collected, or as required by statute/accreditation norms, and securely disposed of thereafter.
- Data Principals (students, staff) may exercise their rights of access, correction, and grievance redressal under the DPDP Act by writing to the University's designated Grievance Officer for data protection.
- Any processing of student or staff data for research, publication, or third-party sharing requires documented consent or another valid lawful basis, and prior clearance from the concerned Dean/Registrar.

9. Physical and Environmental Security

- Server rooms, data centres, and core network equipment shall be housed in access-controlled areas with biometric/card access, fire suppression, and environmental monitoring (temperature, humidity, power).
- Access to server rooms is restricted to authorized IT personnel; visitor access requires prior approval and is logged.
- Critical systems shall be protected by uninterruptible power supply (UPS) and, where feasible, backup generator power, to ensure continuity during outages.
- Decommissioned hardware containing institutional data shall be securely wiped or physically destroyed before disposal or transfer, in line with the data-classification requirements above.

10. Remote Access and VPN

- Remote access to MRV's internal systems (ERP, file servers, administrative applications) is permitted only through an approved, encrypted Virtual Private Network (VPN) or equivalent secure gateway.
- Remote access accounts require Multi-Factor Authentication and are logged and reviewed periodically by IT Services.
- Users shall not use public or unsecured Wi-Fi to access Confidential/Restricted institutional data without VPN protection.

MALLA REDDY VISHWAVIDYAPEETH
Suraram
Hyderabad
(Deemed to be University)

11. Third-Party and Vendor Security

- Vendors and service providers granted access to MRV's network, systems, or data (e.g., ERP vendors, cloud hosting providers, examination-technology partners) must be bound by a written agreement covering data protection, confidentiality, and security obligations equivalent to this policy.
- Vendor access shall be time-bound, logged, and limited to the systems necessary for the contracted service; access shall be revoked promptly on contract closure.
- IT Services shall conduct a security review of any new third-party system prior to integration with MRV's network or data.

12. Cybersecurity Controls

- All endpoints must run University-approved antivirus/endpoint-protection software with automatic signature updates; non-compliant devices may be disconnected from the network.
- Critical data must be backed up on a defined schedule (daily incremental / weekly full, or as prescribed by IT Services), with backups tested periodically and at least one copy held off-site or in the cloud.
- Security patches and OS/application updates must be applied within a defined window of release, prioritized by criticality.
- Firewalls, intrusion detection/prevention systems, and network segmentation shall be maintained to separate academic, administrative, and guest network zones.
- A Disaster Recovery and Business Continuity Plan shall be maintained for critical academic and administrative systems (ERP, examination systems, website), with periodic recovery drills.
- Periodic cybersecurity-awareness training is mandatory for staff and faculty, and shall be incorporated into student orientation, covering phishing, password hygiene, and safe use of digital resources.
- Periodic vulnerability assessment and penetration testing (VAPT) shall be conducted on critical, externally facing systems at least annually.

MALLA REDDY VISHWAVIDYAPEETH
Suraram
Hyderabad
(Deemed to be University)

13. Cyber Incident Response and Reporting

MRV maintains an incident-response process aligned to national requirements, recognizing that a single incident may trigger both cybersecurity and data-protection reporting obligations:

Stage	Action	Timeline
1	Detection / user report of a suspected cyber incident (phishing, malware, unauthorized access, data leak, defacement, etc.) to the IT Helpdesk or CISO	Immediately on discovery
2	Containment and preliminary assessment by IT Services / CISO	Within 2 hours of report
3	Internal escalation to the Vice-Chancellor's office where the incident is significant or involves personal data	Within 6 hours
4	Reporting of the cyber incident to CERT-In, as mandated under Section 70B of the IT Act, 2000 and CERT-In's 2022 Directions	Within 6 hours of detection
5	Where personal data is affected, notification to the Data Protection Board of India and affected individuals, as required under the Digital Personal Data Protection Act, 2023	As prescribed under the DPDP Act and Rules
6	Root-cause analysis, remediation, and closure report to the IT Governance Committee	Within 15 days of containment

14. Bring-Your-Own-Device (BYOD) and Mobile Use

- Personal devices used to access University email, ERP, or other systems must be secured with a screen lock, updated OS, and antivirus protection, and are subject to remote-wipe of institutional data on loss, theft, or separation.
- Use of personal devices for storing Confidential/Restricted institutional data is discouraged; where unavoidable, such data must be encrypted.
- IT Services reserves the right to restrict BYOD access to specific network segments (guest Wi-Fi) separate from the secure administrative network.

MALLA REDDY VISHWAVIDYAPEETH
Suraram
Hyderabad
(Deemed to be University)

15. Video Surveillance

- CCTV surveillance is deployed at entry/exit points, corridors, laboratories, exam halls, classrooms, hostels (common areas only), and other vital points across campus for the safety and security of students, staff, and University property.
- Footage is accessed only by authorized security/administrative personnel and retained for a defined minimum period (as per University protocol) before routine overwrite, except where preserved for an ongoing inquiry or legal proceeding.
- Surveillance does not extend to private spaces such as hostel rooms, washrooms, or changing areas.

16. Social Media and Digital Conduct

- Official University social media accounts are managed only by authorized personnel; personal accounts referencing MRV must not misrepresent official University positions.
- Users shall exercise care not to disclose confidential institutional information, unpublished research, or personal data of others on public or social platforms.

17. Violations and Enforcement

- Violation of this policy may result in disciplinary action under MRV's Code of Conduct/Disciplinary Policy, up to and including suspension of IT access, disciplinary proceedings, or termination/expulsion, in addition to any civil or criminal liability under applicable law.
- Suspected violations should be reported to IT Services or the CISO; department heads are responsible for reporting local violations for institutional action.
- IT Services may temporarily disconnect any device or account posing an immediate security risk to the network, subject to prompt notification to the user/department concerned.

MALLA REDDY VISHWAVIDYAPEETH
Suraram
Hyderabad
(Deemed to be University)

18. Policy Review

This policy shall be reviewed at least once every two years, or earlier upon a significant change in applicable law (including amendments to the IT Act, CERT-In Directions, or the DPDP Act/Rules) or following a major security incident, under the oversight of the IT Governance/Security Committee.

19. Quick-Reference: Do's and Don'ts

Do	Don't
Use strong, unique passwords and enable MFA wherever available	Share your login credentials with anyone, including colleagues
Lock your screen when stepping away from a University system	Leave systems logged in and unattended in shared spaces
Report suspicious emails, links, or devices to IT Services immediately	Click links or open attachments from unknown/suspicious senders
Keep software and antivirus definitions updated	Install unlicensed, pirated, or unapproved software
Back up important institutional data as per the prescribed schedule	Store Confidential/Restricted data on personal devices or drives
Use the official VPN for remote access to internal systems	Access internal systems over public/unsecured Wi-Fi without a VPN
Classify and handle data as per its sensitivity level	Forward institutional data to personal email or third-party apps

Key Contacts

Function	Contact Point
IT Helpdesk (hardware, software, network issues)	University Computer Centre / IT Services Helpdesk
Cybersecurity incidents and CERT-In reporting	Chief Information Security Officer (CISO)
Personal data protection queries and grievances (DPDP Act)	Designated Data Protection Grievance Officer, MRV



Website and official page hosting requests	IT Services / Web Administration Unit
Policy violations and disciplinary referral	Registrar's Office, through the concerned Dean/HOD

MRV reserves its rights to modify, amend, or replace this Policy, including withdrawal, at any time.

— Office of the IQAC / IT Cyber Security Policy, MRV-



Sd/-

Registrar