Vignan's Foundation for Science Technology and Research

(Deemed to be University)

Vadlamudi, Guntur, Andhra Pradesh

Cybersecurity and Data Governance Policy

Version	1.0
Date of Issue	January 2025
Approved By	Board of Management
Academic Year	2024-2025
Classification	Internal / Restricted

1. Policy Statement

Vignan's Foundation for Science Technology and Research (Deemed to be University) is committed to protecting the confidentiality, integrity, and availability of all institutional information assets. This Cybersecurity and Data Governance Policy establishes the framework for managing information security risks, protecting personal data, and ensuring compliance with applicable Indian laws and regulations.

This policy is aligned with the Information Technology Act, 2000 (and its amendments), the Digital Personal Data Protection Act (DPDPA), 2023, and best practices outlined in ISO/IEC 27001:2022 and the CERT-In guidelines.

2. Objectives

- Protect institutional data and information systems from unauthorized access, disclosure, modification, or destruction.
- Ensure continuity of academic and administrative operations through resilient IT infrastructure.
- Establish clear roles and responsibilities for information security across the institution.
- Comply with all applicable national laws and regulatory requirements pertaining to data protection.
- Build a culture of cybersecurity awareness among students, faculty, and staff.

3. Scope

This policy applies to all information assets owned, managed, or operated by the University, including:

- All physical and virtual computing devices (servers, workstations, laptops, tablets, smartphones).
- Network infrastructure including wired, wireless, and cloud-based systems.
- All software applications including ERP, LMS, email, and web portals.
- All categories of data: student records, financial data, research data, HR records, and communications.
- All personnel: employees, students, contractors, vendors, and visiting researchers.

4. Information Classification

All institutional information shall be classified into the following categories:

Classification	Description	Examples
Confidential	Highly sensitive; access strictly restricted	Financial records, legal documents, exam papers, HR data
Restricted	Sensitive; limited access on need-to-know basis	Student personal data, research data, system configurations

Classification	Description	Examples
Internal	For internal use; not for public disclosure	Policies, meeting minutes, internal reports
Public	Approved for public release	Prospectus, annual reports, public website content

5. Access Control

- All systems shall enforce Role-Based Access Control (RBAC) limiting access to the minimum necessary for job functions.
- User accounts shall be created based on formal authorization from the relevant departmental head.
- Privileged access (system administrator rights) shall be restricted, logged, and reviewed quarterly.
- Multi-Factor Authentication (MFA) shall be mandatory for all administrative and remote access.
- User accounts shall be deactivated within 24 hours of separation from the University.

6. Password and Authentication Policy

- Passwords shall be a minimum of 8 characters containing uppercase, lowercase, numerals, and special characters.
- Passwords shall be changed every 90 days and must not be reused for the last 10 cycles.
- Default system passwords shall be changed immediately upon deployment of any new device or application.
- Password storage shall use industry-standard hashing algorithms (sha512 or md5).

7. Network Security

- The University network shall be segmented into zones: academic, administrative, guest, and research.
- All network traffic between zones shall pass through a managed firewall with defined rule sets.
- Intrusion Detection and Prevention Systems (IDS/IPS) shall be deployed at network perimeters.
- Guest Wi-Fi shall be isolated from internal institutional networks.
- All remote access shall be through encrypted Virtual Private Network (VPN) connections.

8. Data Protection and Privacy

8.1 Personal Data Protection

In accordance with the Digital Personal Data Protection Act (DPDPA), 2023, the University shall:

- Collect personal data only for specified, explicit, and legitimate purposes.
- Obtain explicit consent from data principals before processing personal data.
- Implement data minimization principles, collecting only what is necessary.
- Provide data principals with the right to access, correct, and erase their personal data.
- Appoint a Data Protection Officer (DPO) responsible for DPDPA compliance.

8.2 Data Breach Response

- Any suspected data breach shall be reported to the CISO within 2 hours of discovery.
- CERT-In shall be notified of reportable incidents within 6 hours as mandated by law.
- Affected data principals shall be notified within 72 hours of confirmed breach.
- A post-incident review shall be conducted within 30 days of every breach.

9. Endpoint and Device Security

- All University-owned devices shall have licensed antivirus and endpoint protection software.
- Operating systems and applications shall be patched within 30 days of patch availability.
- Full-disk encryption shall be enabled on all laptops and portable storage devices.
- Use of personal devices to access institutional systems is subject to Mobile Device Management (MDM) enrollment.
- Unauthorized installation of software on University devices is prohibited.

10. Incident Management

- The University shall maintain a documented Incident Response Plan (IRP) tested annually.
- A Computer Security Incident Response Team (CSIRT) shall be constituted with defined roles.
- All security incidents shall be logged in the incident management system.
- Incidents shall be classified by severity and responded to within defined SLA timelines.

11. Security Awareness and Training

- All new employees and students shall complete mandatory cybersecurity awareness training within 30 days of joining.
- Annual refresher training shall be conducted for all staff.
- Simulated phishing exercises shall be conducted at least twice a year.
- Security awareness materials shall be displayed across campuses and digital channels.

12. Audit and Compliance

- An annual Information Security Audit shall be conducted by an independent agency.
- Vulnerability Assessment and Penetration Testing (VAPT) shall be performed twice a year.
- Audit findings shall be reported to the IQAC and Board of Management.
- Corrective actions shall be implemented within 90 days of audit completion.

13. Sanctions and Enforcement

Violations of this policy may result in disciplinary action including suspension of system access, departmental action, and legal proceedings under applicable Indian laws including the IT Act, 2000.

14. Review

This policy shall be reviewed annually or immediately following any significant security incident, regulatory change, or major technology deployment.

(Dr. Y Ravi Sekhar)
Dean, Technology & Development

DEAN
Technology Development
VFSTR Deemed to be University
Vadlamudi-522 213, Guntur (Dt.)