विज्ञानं ब्रह्म

Shri Mata Vaishno Devi University

Kakryal, Katra–182320 (J&K) INDIA
(A State University recognized u/s 2(f) & 12(B) of UGC)

Ref No. SMVDU/NC/2025/1404-09 Date: 31.10.2025

Notification

Subject: Implementation of Comprehensive IT Policy at SMVDU.

As approved by the Competent Authority, the comprehensive IT policy of the University is notified for information and compliance.

This policy outlines clear guidelines for:

- Proper usage of University IT resources and infrastructure.
- Data security, privacy, and confidentiality measures.
- Network and internet usage norms.
- Software licensing and intellectual property compliance.
- Cybersecurity practices and incident reporting procedures.
- Imposition of penalties for damage or misuse of network equipment.

A copy of the IT policy is appended herewith.

All faculty, staff and students of the University are required to strictly adhere to the provisions of this IT Policy. Any non-compliance shall invite disciplinary actions in accordance with University rules and regulations.

This issues with the approval of the Competent Authority.

Registrar

Enclosure: As above.

1. All Deans/Heads/Section Heads for information and circulation among faculty, staff and students for compliance.
2. PS to VC, for kind information of the Hon'ble Vice-Chancellor.
3. Finance Officer, for kind information.
4. Notification/Order File.
5. I/C website for uploading of IT Policy in SMVDU website.

Comprehensive IT Policy
Shri Mata Vaishno Devi University

Contents

Comprehensive IT Policy
Shri Mata Vaishno Devi University

Introduction and Objectives

Shri Mata Vaishno Devi University (SMVDU) is committed to the efficient, secure, and lawful use of Information Technology resources in pursuit of its academic and administrative mission. This **Information Technology (IT) Policy** establishes guidelines and a governance framework for all users of the University's IT assets. The policy aligns with India's national and regulatory frameworks – including the Information Technology Act, 2000 (Amended 2008), the Digital Personal Data Protection (DPDP) Act, 2023, CERT-In cybersecurity directives, University Grants Commission (UGC) and AICTE guidelines, the National Education Policy (NEP) 2020 digital vision, and initiatives like Digital India and MeitY's MeghRaj cloud program. The objectives of this policy are to:

- **Protect** the confidentiality, integrity, and availability of University data and IT systems.
- **Ensure Compliance** with all applicable laws, regulations, and standards in IT usage.
- **Enable Academic Innovation** by providing robust and modern digital infrastructure in line with NEP 2020's vision for open and evolvable educational technology.
- **Promote Responsible Use** of IT resources by all stakeholders through clear rules, awareness, and accountability.

Scope and Applicability

This policy applies to **all users** of SMVDU's IT resources, including but not limited to: students, faculty, researchers, administrative staff, contractual employees, third-party service providers, vendors, consultants, and external collaborators. It covers all University-owned or managed IT assets (networks, servers, computers, mobile devices, software, cloud services, data, and communication systems) as well as personally-owned devices (BYOD) when used to access University networks or data. **Acceptance of this policy** is a condition of access to University IT resources. All users and affiliated third parties must:

- Abide by the rules and procedures outlined herein when accessing or using SMVDU's IT systems.
- Protect University data they handle as per its classification (Public, Confidential, Sensitive).
- Ensure that any personal devices used on campus networks comply with University security standards (up-to-date OS, antivirus, no unauthorized software).

- Acknowledge that violation of this policy may result in disciplinary action and/or revocation of access.

External partners or vendors with whom University data is shared must sign appropriate agreements binding them to **equivalent data protection and IT security standards** as described by this policy. These standards ensure that third parties also comply with Indian IT laws and data protection regulations when handling University information.

IT Governance and Oversight

IT governance at SMVDU is structured to provide strategic direction, ensure accountability, and manage risk in the use of technology. A cross-functional **IT Steering Committee** shall oversee major decisions, compliance monitoring, and resource allocation for IT. This committee, chaired by a senior executive (e.g. the Vice Chancellor or a nominee), meets regularly (at least annually) to review IT strategy and policy adherence. Key roles and bodies include:

- **IT Steering Committee:** Sets IT strategy and approves policies; reviews major IT investments; monitors compliance and risk at a high level.
- **Director of IT / Network Centre Head:** Responsible for policy implementation, day-to-day IT operations, and security oversight. This role includes conducting audits, leading incident response, and advising on infrastructure improvements.
- **Registrar (or Compliance Officer):** Ensures institutional compliance with legal and regulatory requirements. The Registrar oversees disciplinary processes for policy violations and coordinates with the HR and student affairs departments on enforcement.
- **Data Protection Officer (DPO):** A DPO shall be appointed as required under the DPDP Act 2023 to oversee personal data protection practices. The DPO monitors compliance with data privacy laws, conducts data protection impact assessments, and addresses grievances related to personal data.
- **Systems and Network Administrators:** Technical staff who implement security controls, manage user accounts, maintain hardware/software, and uphold this policy's technical standards.
- **Departmental IT Coordinators:** Representatives in various faculties or departments who liaise with the IT department to ensure local needs are met and policies followed.

All governance decisions will be documented. The IT Steering Committee will provide an **annual report** on the state of IT at the University, summarizing key initiatives, compliance status, incidents, and recommendations for improvements.

Legal and Regulatory Compliance

SMVDU shall adhere strictly to **all applicable IT-related laws and regulations of India**, ensuring that University IT practices reflect the latest legal requirements:

- **Information Technology Act, 2000 (Amended 2008):** All IT usage must comply with the IT Act and its amendments, which form the foundation of India's cyber law framework. Activities that constitute offenses under the Act (such as hacking, identity theft, cyber terrorism, obscene content, etc.) are strictly prohibited on University systems. Users must not engage in any act that could subject the University or themselves to liability under this Act. The University will cooperate with law enforcement as required under sections dealing with monitoring, interception or cybercrime investigations, in accordance with due process.
- **Digital Personal Data Protection Act, 2023:** As a data fiduciary under the DPDP Act, SMVDU is committed to protecting personal data of students, employees, and other individuals. Personal data will be processed only for lawful purposes with consent or other permitted basis, and users ("data principals") have rights to access, correct, and erase their digital personal data. The University shall provide clear notices when collecting personal information and obtain consent where required. A grievance redressal mechanism will be in place for individuals to report data privacy concerns. In compliance with the Act, a Data Protection Officer will oversee data handling practices and ensure **security safeguards and transparency** in data processing. In the event of a personal data breach, SMVDU will notify the concerned authorities (such as the Data Protection Board of India) and affected individuals in the prescribed manner.
- **CERT-In Cybersecurity Guidelines (2022):** The University abides by the cybersecurity directives issued by the Indian Computer Emergency Response Team (CERT-In). This includes the mandatory 6-hour reporting window for certain cybersecurity incidents and breaches to CERT-In, and maintenance of ICT system logs within Indian jurisdiction for a minimum of 180 days. All required cyber incidents (as listed by CERT-In) will be reported to the government authorities in a timely fashion. The University's network and security team will ensure log retention and time synchronization as per CERT-In rules to aid in investigations and compliance.
- **UGC/AICTE Guidelines:** SMVDU's IT usage is guided by UGC and AICTE recommendations on ICT in higher education. The University acknowledges UGC's "Cybersecurity for Higher Education Institutions" handbook, which emphasizes user awareness, strong passwords, phishing prevention, and prompt reporting of cyber incidents. In line with these guidelines, SMVDU conducts regular cybersecurity awareness programs and has implemented

robust measures such as network firewalls, encryption of sensitive data, and periodic system updates.

- **National Education Policy 2020:** The policy aligns with NEP 2020's digital infrastructure vision, which calls for investment in **open, interoperable, evolvable public digital infrastructure** for education. SMVDU supports the NEP's emphasis on leveraging technology for teaching, learning, and administration while addressing the digital divide and data privacy. This translates into adopting modern e-learning platforms, digital repositories, and online assessment tools in a secure and equitable manner (see "Academic and Research Technology Use" below).
- **Digital India and MeitY's MeghRaj Cloud Initiative:** In support of the Digital India mission, the University seeks to optimize IT costs and improve e-services by smart use of cloud computing. Following MeitY's MeghRaj (GI Cloud) guidelines, SMVDU favors cloud services that store data in-country and comply with government security standards. Any cloud service engaged (for instance, for ERP or learning management) must either be empanelled by MeitY or meet equivalent security and data residency requirements. This ensures that University data on cloud platforms is protected by contracts and technical controls consistent with national policy.

Additionally, SMVDU will comply with other relevant statutes such as the **Indian Penal Code / Bharatiya Nyaya Sanhita (as applicable to cybercrimes)**, the **Copyright Act (digital content usage)**, and the **Rights of Persons with Disabilities (RPWD) Act, 2016** for accessible IT services. All procurement of IT products will consider Section 46 of the RPWD Act, which mandates ICT accessibility for persons with disabilities.

Compliance Assurance: The University will conduct periodic reviews to verify that IT practices remain in compliance. Any updates or new regulations (for example, new CERT-In advisories, rules under DPDP Act, etc.) will be incorporated into this policy promptly. Users will be informed of their responsibilities under these laws through trainings and communications.

Infrastructure and Network Management

SMVDU is dedicated to providing a reliable, high-performance, and secure IT infrastructure. This section outlines policies for managing the University's hardware, software, networks, and cloud resources:

1. IT Infrastructure Lifecycle: All IT hardware and software shall be acquired, maintained, and retired following standardized procedures:

- **Procurement:** IT equipment and services will be procured in line with Government of India guidelines (e.g., via GeM – Government e-Marketplace –

and giving preference to “Make in India” products where feasible). Technical evaluation must ensure that new systems meet security and interoperability standards.

- **Inventory and Asset Management:** The IT department will maintain an inventory of all IT assets. Each asset will have a lifecycle plan including maintenance schedules, warranty tracking, and end-of-life (EOL) disposition. Obsolete or unserviceable IT assets will be disposed of in compliance with e-waste management rules and environmental guidelines.
- **Upgrades and Modernization:** The University will plan for regular upgrades of network bandwidth, servers, and end-user devices to meet growing academic needs. A **hardware refresh cycle** (e.g., every 4-5 years for servers/network equipment, 5-6 years for desktops) will be observed to prevent performance degradation and security risks from outdated equipment.
- **Redundancy and Continuity:** Critical infrastructure (such as data center servers, network core, and storage) shall have redundancy (backup hardware or failover arrangements) to achieve high availability. Power backup (UPS, generator) must support key IT facilities. An **Infrastructure Disaster Recovery (DR) plan** will define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical systems in case of major outages. Off-site or cloud backups may be used to meet DR requirements.

2. Network Management: The University network (wired and wireless) is a vital resource that must be well-managed to ensure connectivity, security, and performance for all users:

- **National Knowledge Network (NKN) Integration:** SMVDU’s campus network is connected to high-speed National Knowledge Network links (and other ISPs like BSNL). Bandwidth allocation and traffic routing will be optimized to prioritize academic and research activities. The network team will coordinate with NKN/ISP for uptime and capacity upgrades as needed.
- **Bandwidth and Quality of Service (QoS):** The available internet bandwidth will be distributed fairly. QoS rules may be applied to ensure critical services (e.g., ERP, online classes, library resources) get priority over recreational traffic. The University targets an uptime SLA of 99.5% or higher for core network services. Any planned downtime for maintenance will be announced in advance.
- **Wireless Networks:** Secure Wi-Fi will be provided in academic blocks, hostels, and other campus areas. Separate SSIDs or network segments may be used for different user groups (students, faculty, guests) to enforce appropriate access controls. **Guest access** for visitors shall be time-limited and isolated from internal systems.

- **Network Security:** A **Next-Generation Firewall (e.g., Sophos)** is deployed at the campus perimeter to protect against external threats and to filter malicious or unauthorized traffic. The firewall and associated systems (IDS/IPS, web filtering, anti-malware gateway) will be configured to block attacks, malware, and access to prohibited content in accordance with law and University policies. The firewall also enables monitoring of network traffic and enforcement of internet usage rules (for example, blocking pornography, piracy, hate sites, etc., as per Government and regulatory guidelines). The UGC advises institutions to implement such robust measures like firewalls and regular system updates to minimize cyber risks.
- **IP Address Management:** The IT department will manage IP address allocation (through DHCP or static assignment as needed). Users must not set unauthorized static IPs or alter network equipment. Any addition of networking devices (like routers, switches, access points) must be approved by the Network Centre.
- **Network Usage Policy:** Users are expected to use the network primarily for academic, research, and administrative purposes. Limited personal use is permitted (see "Email and Communication" section), but **commercial use of the University network is strictly prohibited** without explicit authorization. Activities that strain network resources (e.g., excessive downloading, hosting servers, crypto-mining, etc.) or violate copyrights are forbidden. The University may throttle or block traffic that adversely impacts network performance or legal compliance.
- **Remote Access:** Remote access to the University network (for example, via VPN) will be provided to authorized users for legitimate purposes (like accessing internal systems from off-campus). Strong authentication (2FA) and encryption must be enforced for all remote connections. All remote access is logged.

3. Software and Application Management:

- **Licensed Software:** All software installed on University systems must be properly licensed or open-source. Users must not install pirated or unauthorized software. The IT department will maintain site licenses for common software (operating systems, productivity suites, anti-virus, etc.) and provide approved software through official channels.
- **Software Updates and Patches:** The IT team will regularly apply security patches and updates to servers, network devices, and institution-provided client machines. Automatic update features should be enabled where possible. Users of personal devices are responsible for keeping their systems updated when connected to the University network.

- **Web Applications and Portals:** University web applications (such as the official website, Samarth ERP, LMS, etc.) shall be developed and maintained following secure coding practices. Regular vulnerability assessments will be conducted on these applications. All official web content must adhere to government web guidelines (GIGW) and be accessible (WCAG 2.1 compliance for web accessibility).
- **Cloud Infrastructure:** Cloud servers or services (IaaS/PaaS/SaaS) used by the University must be authorized by the IT department. Data stored in cloud services should have proper backups and security controls. Preference is given to cloud offerings under MeitY's MeghRaj or those empanelled by the government for use by educational institutions, to ensure data is hosted in India and meets compliance standards.

4. Data Center and Physical Security:

- The University's central IT facilities (data centers, server rooms) shall have controlled access – only IT staff and authorized personnel are allowed entry. These facilities must have environmental controls (adequate cooling, power surge protection, fire suppression) and physical security measures (CCTV monitoring, biometric or smart card access locks).
- Critical servers will have backup power. Regular backups of critical data are mandatory – with both onsite and offsite (or cloud) backup schedules. Backup integrity will be tested periodically. The backup policy will define retention periods (e.g., daily backups kept for 30 days, monthly backups for 1 year, etc.) in accordance with data retention requirements.

5. High-Availability (HA) Architecture Policy

To minimize outages and single points of failure, SMVDU shall operate critical network and data-centre components in **High-Availability (HA)** mode:

- **Perimeter firewall**: deploy a redundant firewall pair (active–standby or active–active) with stateful failover; failover test at least quarterly in a scheduled maintenance window.
- **Core switching & routing**: dual core switches with redundant uplinks (link aggregation where feasible); distribution to critical buildings on diverse paths.
- **Virtualization & storage**: clusterized compute and redundant storage controllers; shared storage with multipath I/O; hot-spare capacity sized for N+1 resiliency.
- **Power & facilities**: dual UPS feeds for data-centre racks; generator backup tested monthly; environmental monitoring with alerting.
- **Change control**: any HA failover or firmware upgrade occurs in maintenance windows with a backout plan; change records stored in the IT helpdesk/CMDB.

6. E-Waste Management

SMVDU shall implement an immediate and continuous e-waste program:

- **Inventory & segregation** of obsolete/unserviceable IT assets; recording in the asset register.
- **Disposal** strictly as per E-Waste (Management) Rules via CPCB-authorized recyclers, including data-sanitization certificates (secure wipe/degauss/shred for storage media).
- **Governance**: appoint a Nodal Officer for e-waste; publish a half-yearly summary of disposals.
- **Moratorium**: no storage of obsolete equipment beyond 90 days after condemnation proceedings.
- **Awareness**: campus communication on responsible disposal; no informal resale or scrap outside approved channels.

7. Hardware Upgrades & Modernization

- **Refresh target**: prioritize Network Centre devices (servers, firewalls, switches, storage, backup) that are EoL/EoS (7–15 years old) for replacement.
- **Budgeting**: plan procurement of latest, standards-compliant technology within one year of the enforcement of this policy, giving preference to MeitY-empanelled/cloud-ready solutions.
- **Lifecycle**: adopt a rolling 4–5 year refresh for core infrastructure thereafter.

8. Internet Connectivity Redundancy

- Contract a second 1 Gbps Internet link from an alternate ISP and configure automatic failover/BGP to ensure resilience against provider or last-mile faults; target implementation within one year of the enforcement of this policy.
- Maintain path diversity (separate PoEs/ducts where feasible); test failover quarterly.

Overall, the Infrastructure and Network Management policy ensures that SMVDU's IT environment is robust, up-to-date, scalable, and secure, providing a foundation for all academic and administrative computing needs.

Cybersecurity and Incident Response

SMVDU recognizes cybersecurity as a critical priority. This section defines how we protect our information assets and respond to security incidents:

1. Information Security Program: The University will maintain a comprehensive Information Security Program aligned with industry best practices and standards (such as ISO 27001). This includes periodic risk assessments to identify threats and vulnerabilities, and implementation of controls to mitigate risks. Areas of focus include access control, network security, malware protection, data security, and incident management.

2. Security Policies and Controls: Key cybersecurity measures in place:

- **Authentication & Identity Management:** All user accounts (for systems like Samarth ERP, Google Workspace, etc.) will be secured with strong authentication. The University has implemented Single Sign-On (SSO) via Google Workspace for many services, and **Two-Factor Authentication (2FA)** is **mandatory** for all privileged users and strongly encouraged for all accounts. Administrators and faculty/staff accounts with access to sensitive data must use 2FA without exception. Passwords must meet complexity requirements and be changed periodically (at least every 90 days). The password policy requires a minimum length, mix of character types, and disallows reuse of recent passwords. Account lockout thresholds are set to deter brute-force attacks. **Sharing of passwords** or login credentials is prohibited; users are accountable for actions performed through their credentials.
- **Endpoint Protection:** All University-owned computers and servers must run up-to-date anti-virus/anti-malware software. The IT department manages a centralized Endpoint Detection and Response (EDR) solution to detect and isolate malware, ransomware, or suspicious activities on endpoints. Users are expected not to disable or tamper with security software. Personal devices connecting to the network should also have updated anti-malware protection and adhere to best practices; the University may scan devices for compliance before granting network access (especially for BYOD connecting to internal systems).
- **Network Defense:** The **Sophos Firewall** (or equivalent) provides intrusion prevention, content filtering, and traffic monitoring at the network perimeter. It inspects inbound and outbound traffic to block attacks, viruses, and unauthorized access attempts. Internal network segmentation is used to contain potential breaches (e.g., separating student labs, administrative networks, and server subnets). Wireless networks use WPA2/WPA3 encryption and client isolation as appropriate.
- **Secure Configuration:** Servers and network devices are hardened as per guidelines (disabling unnecessary services, using firewalls, strong admin passwords, etc.). Default passwords are changed and administrative interfaces are secured. The IT team will benchmark configurations against security standards and perform regular audits.

3. Cybersecurity Awareness: A strong security posture requires vigilant users. The University conducts regular **training and awareness programs** (detailed later in Training and Awareness) to educate users about phishing, social engineering, safe browsing, and data protection. All users must exercise caution with emails and online communication – particularly with attachments or links – to avoid falling victim to phishing or malware. The UGC's cybersecurity handbook's recommendations on recognizing phishing and using strong passwords are emphasized in these trainings.

4. Incident Response Plan (IRP): Despite preventive measures, security incidents may occur. SMVDU has a defined **Cybersecurity Incident Response Plan** to handle such events promptly and effectively. Key elements include:

- **Incident Classification:** Incidents will be categorized by severity and type (e.g., Critical – major breach or widespread service outage; High – significant malware infection; Moderate – isolated compromise; Low – minor violation or false alarm). This classification guides the urgency of response.
- **Reporting Mechanism:** All users must immediately report any suspected cybersecurity incident or weakness to the IT Security Team. A dedicated incident reporting channel (such as a security email address or a module in the Samarth portal) will be provided for confidential reporting of incidents like phishing attempts, lost devices, suspected breaches, etc.. The University commits to protecting whistleblowers who report security issues in good faith.
- **Response Team:** An Incident Response Team (IRT) led by the Director of IT (or a designated Information Security Officer) will convene for confirmed incidents. The team may include system admins, network admins, the DPO (if personal data involved), and representatives from management or communications as needed. The IRT will follow a structured process: Detect -> Contain -> Eradicate -> Recover -> Review.
- **Containment and Recovery:** Upon a security incident, immediate steps will be taken to contain the impact. For example, isolating affected systems from the network, resetting passwords, applying patches or fixes, and restoring data from backups if needed (in case of ransomware or data corruption). The University's disaster recovery resources will be invoked if an incident disrupts critical services (e.g., switching to backup servers).
- **Forensics and Investigation:** The IT team will preserve relevant logs and evidence of the incident. Where appropriate, affected systems may be forensically analyzed to determine the cause and extent of compromise. The University may involve external cybersecurity experts or CERT-In for major incidents requiring advanced analysis.
- **Incident Reporting and Escalation:** In line with CERT-In's 2022 directive, certain incidents (like large-scale breaches, critical system compromises, ransomware attacks, etc.) **must be reported to CERT-In within 6 hours of detection**. The IRT will ensure compliance with this reporting requirement by preparing and sending incident reports with the required details. Concurrently, internal escalation will happen – critical incidents will be communicated to University leadership (Registrar, Vice Chancellor) immediately, along with actions being taken. Law enforcement will be contacted if any criminal activity is suspected (for instance, cyberattacks originating externally or involving illegal content).

- **Communication:** During a significant incident, transparent communication with stakeholders is vital. The University will inform affected parties without undue delay – e.g., if student or employee data is leaked, those individuals will be notified with guidance on next steps (in accordance with DPDP Act breach notification norms). Public or media statements (if needed) will be handled by authorized officials to ensure accurate information.
- **Post-Incident Review:** After resolving an incident, the IRT will document a report detailing the root cause, extent of damage, and mitigation steps taken. A **post-incident review meeting** will identify lessons learned and recommend improvements to prevent similar incidents. Any gaps in controls will be addressed promptly (for example, updating firewall rules, user training refreshers, etc.). If the incident revealed policy weaknesses, those will be considered in the next policy review.

5. Threat Intelligence and Monitoring: The University's IT team will subscribe to threat intelligence feeds (such as CERT-In advisories, vendor security bulletins) to stay updated on emerging cyber threats. Proactive measures like regular vulnerability scanning of University systems and penetration testing (at least annually or after major changes) will be carried out to uncover and fix security weaknesses. A Security Information and Event Management (SIEM) system will be used to aggregate logs from various sources (firewall, servers, etc.) and alert on suspicious patterns. These logs will be retained as mandated (minimum 180 days) and reviewed periodically to detect any anomalies.

6. Acceptable Use and Prohibited Activities: Cybersecurity also entails clearly defining what users should not do:

- Users shall not engage in unauthorized access of any system (hacking) or attempt to exploit vulnerabilities. This includes port-scanning, sniffing network traffic, or using another person's credentials. Such actions are illegal under the IT Act and strictly forbidden.
- The introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses) is prohibited. Intentional creation or propagation of malware will result in severe disciplinary action.
- Users must not disable or circumvent security controls (firewall, antivirus, access controls) installed on their devices or the network.
- Personal network devices (like Wi-Fi routers) should not be connected to the University network without IT approval, as they may bypass security controls.
- **Data Confidentiality:** Users who handle sensitive data (research data, exam papers, personal information) must take precautions such as encryption and secure storage. They should not copy such data onto insecure devices or cloud accounts not approved for use.

- **Reporting Obligation:** If a user inadvertently causes or discovers a security issue, they are expected to report it and not conceal it. The goal is remediation, not blame – minor unintentional violations reported promptly may be treated leniently, whereas willful neglect or malicious intent will face full sanctions.

7. Network Security Access Policy (Allow/Block)

The University network is for **academic, research, and administrative** purposes. The firewall policy shall:

- **Allow**: institutional portals (Samarth ERP, LMS, library resources), research/academic sites, scholarly repositories, verified software sources, and approved collaboration tools.
- **Restrict/Block**: malware, pornography, piracy, violent/extremist content, crypto-mining, P2P/torrent protocols (unless pre-approved for research), anonymizers/VPNs that bypass security, high-risk file-hosting, and any site/app deemed harmful or non-academic.
- **Exceptions**: department HoD/PI may request temporary exceptions with academic justification; IT records exception approvals, scope, duration, and responsible user(s); logs are reviewed.
- **Reviews**: category lists updated monthly; rule changes tracked in change control.

8. Endpoint Security & Awareness Program

To address the current gap of no centralized endpoint protection:

- Mandatory Endpoint Protection (EDR/AV) for all University-owned endpoints and servers; BYOD devices must meet minimum posture (patched OS, AV) before internal access (NAC posture check where feasible).
- **Central console** for policy enforcement, tamper protection, and incident isolation.
- **User awareness**: semester-wise phishing drills; annual mandatory cyber-hygiene training for all users; targeted refreshers for high-risk roles.
- **Disaster Recovery**: maintain image-based backups for critical servers and configuration backups for network/security devices; DR tests at least **annually**.

9. Security Information & Event Management (SIEM)

- **Implement a SIEM** (e.g., **Splunk/IBM QRadar/FortiSIEM**) within one year of the enforcement of this policy; integrate logs from firewalls, servers, endpoints, IAM/SSO, ERP/LMS, Wi-Fi controllers.
- **Compliance**: retain logs ≥180 days in-country; time-sync (NTP), alert triage runbooks, and quarterly use-case tuning.

10. Dedicated Storage & Encryption

- Stand up dedicated storage infrastructure (SAN/NAS or cloud) with encryption at rest, access controls, snapshots, and replication.
- Enforce TLS in transit; protect encryption keys (HSM/KMS or provider-managed keys with strict admin separation).
- Backups follow 3-2-1 principle with periodic restore testing; classify data and apply stronger controls to confidential/sensitive classes.

By implementing the above measures and fostering a culture of vigilance, SMVDU aims to minimize cybersecurity incidents and be prepared to respond effectively when they occur, thereby protecting both individual and institutional digital assets.

Data Privacy and Protection

The University highly values data privacy and is dedicated to handling personal and institutional data with due care and in compliance with the DPDP Act 2023 and other privacy regulations. This section details how data is classified, stored, and protected:

1. Data Classification: All University data shall be classified into categories to determine the required security controls and handling procedures:

- **Public Data:** Information intended for public consumption. E.g., press releases, campus event information, published research open to all, website content. This data requires minimal security but must still be accurate and protected from unauthorized modification.
- **Internal/Official Data:** Non-public data that is for internal University use. E.g., internal memos, policy documents, most academic course materials. Moderate security controls (access for authorized users only) are applied.
- **Confidential Data:** Sensitive data that could harm individuals or the University if disclosed. E.g., student academic records, exam questions, employee HR records, research in progress, financial data. Access to confidential data is restricted to authorized personnel on a need-to-know basis, and such data must be stored in secure systems.
- **Highly Sensitive Data (Protected Data):** This includes **personal identifiable information (PII)** such as Aadhaar numbers, financial information, medical records of students/staff, passwords/credentials, and any data classified as sensitive personal data under law. Also, certain research data under embargo or government projects might fall here. This data requires the highest level of protection – encryption at rest and in transit, strict access logs, and often explicit consent from the data principal for its collection/use.

Each department or data owner is responsible for labeling and handling data according to these classifications. The IT department provides tools (like secure file storage and encryption) to assist in protection.

2. Personal Data Protection (DPDP Act Compliance): In collecting and processing personal data, SMVDU adheres to the principles of lawfulness, purpose limitation, and data minimization:

- **Consent and Notice:** Wherever feasible, the University will obtain consent from individuals (students, staff) before collecting their personal data, especially sensitive data (e.g. health details, biometric attendance data). Consent notices will be clear, describing the purpose of data use. For example, at the time of student admission or staff onboarding, a privacy notice and consent form will be provided.
- **Purpose Limitation:** Personal data collected for a specific purpose (admission, exam administration, library use, etc.) will not be used for other purposes without additional consent or a valid legal basis.
- **Data Minimization:** Only the data necessary for a given function will be collected. Extraneous personal information will be avoided.
- **Data Accuracy:** The University will maintain personal data accurately and update it as needed. Individuals are encouraged to use self-service in Samarth ERP to keep their contact and personal details current.
- **Data Retention and Erasure:** Personal data will be retained only as long as necessary for the purpose it was collected or as mandated by law (for example, examination records may be kept for a number of years as per academic regulations). Once data is no longer needed, it will be securely disposed of or anonymized. Individuals have the right to request deletion or correction of their personal data, and the University will honor such requests in line with applicable law (subject to any legal retention requirements).
- **Children's Data:** Although University students are generally adults, if any personal data of minors (under 18) is processed (e.g., participants in an outreach program or child of an employee), parental consent will be obtained as required by DPDP Act. Any data pertaining to minors will not be processed in a way that is harmful or for any tracking/advertising purposes.

3. Data Storage and Encryption:

- **Encryption:** Sensitive and confidential data stored on University systems (servers, databases, laptops) must be encrypted at rest where technically feasible, especially on portable devices. Full-disk encryption is mandated for laptops containing confidential data. All data in transit over networks (between client and server or between servers) should be encrypted using protocols like HTTPS, SSL/TLS, or VPN tunnels.

- **Secure Storage Solutions:** Official data should be stored on approved servers or cloud services (such as the University's Google Drive under Workspace, or on-premise file servers) which have proper access control and backup. Avoid storing University confidential data on personal cloud accounts or USB drives without permission.
- **DigiLocker/NAD Integration:** In alignment with Digital India, SMVDU utilizes government-backed secure repositories for certain data. For instance, student academic certificates and transcripts may be deposited in the **National Academic Depository (NAD)** or the **Academic Bank of Credits (ABC)** system and made available through DigiLocker for secure access by students and verifiers. This ensures verifiable credentials storage in a tamper-proof manner. The IT policy supports integration with these national systems to protect authenticity and confidentiality of academic records.

4. Data Access Controls: Access to University data is governed by the principle of least privilege:

- Each user is granted the minimum access required for their role (see Role-Based Access Control in a later section). For example, a faculty member can access data for their students but not all students in the University; a clerk in admissions can view applicant data but not employee salaries.
- Sensitive databases (like the student information system, finance system) have role-based modules and require individual authenticated logins. Generic or shared accounts are avoided; if used, they must be tightly controlled and logged.
- Before granting third-party service providers access to any sensitive data (for software support, cloud processing, etc.), a Data Sharing Agreement or Non-Disclosure Agreement must be in place outlining privacy requirements and liabilities.

5. Data Breach Notification and Response: Despite best efforts, if a data breach is suspected or confirmed (e.g., personal data is accessed by unauthorized person, lost, or stolen):

- The incident must be reported immediately to the IT Security Team and the DPO. An investigation will be conducted as per the Incident Response Plan.
- If a breach involving personal data is confirmed, the University will notify the affected individuals expeditiously, advising them of the nature of data involved and steps to protect themselves (such as changing passwords, watching for fraud). Such notification will occur within 48 hours of confirming the breach or as mandated by law.

- The University will also fulfill any legal reporting obligations – e.g., report the breach to the Data Protection Board of India or CERT-In, if required, with all necessary details.
- Remedial measures will be taken immediately to contain and mitigate the breach (like disconnecting compromised systems, invoking backups). Post-breach, a root cause analysis will be done and controls improved to prevent recurrence.

6. Data Audits and Privacy Assessments:

- The DPO or an appointed auditor will conduct periodic **data protection audits** to ensure compliance with the DPDP Act and this policy. This includes checking if consents are recorded, data is properly classified, and only necessary data is being stored.
- New projects or systems involving personal data undergo a Privacy Impact Assessment to evaluate risks and required safeguards before launch.

7. User Privacy Expectations: The University respects the privacy of user communications and files; however, it must balance this with institutional security needs. **Users should be aware that there is limited expectation of privacy** when using University IT resources for the following reasons:

- The University may monitor network traffic, email, and system usage for security, maintenance, or legal compliance purposes. Any such monitoring is done by authorized personnel and in accordance with applicable laws and regulations.
- Access to user data by administrators will be strictly controlled – e.g., for troubleshooting or investigations, and will require approval from competent authority (Registrar or DPO) except in emergencies. All administrative access to user accounts or data will be logged and auditable.
- The University will not access personal content of users (like personal emails or files) without consent, **except** when required by law, investigation of policy violations, or pressing security concerns. Even in such cases, the principle of least perusal is followed (only accessing information directly pertinent to the issue).
- The DPDP Act gives individuals rights over their data; the University is committed to honoring those rights. Users can contact the DPO to inquire about their stored personal data or request corrections/deletions, and such requests will be processed as per legal provisions.

In summary, SMVDU's data protection practices ensure that personal and sensitive information is collected and used responsibly, kept secure through technical and organizational measures, and that individuals' privacy rights are respected in

accordance with Indian law. All community members handling such data share in the responsibility to protect it.

Email and Communication Policy

This section governs the use of University-provided email and communication tools (e.g., Google Workspace Gmail, calendars, chats) as well as expectations for electronic communications:

1. Official Email Usage: All students, faculty, staff, and authorized associates are provided with an official SMVDU email account (typically @smvdu.ac.in via Google Workspace). Official email is the primary channel for University communications. Users **must use their SMVDU email** for all university-related correspondence. Important announcements, circulars, and individual notices (e.g., exam schedules, fee reminders, HR notices) will be sent to these official addresses, and users are expected to check their email regularly. Using official email ensures authenticity and compliance, as messages are archived and under University control.

2. Personal Use of Email: Incidental personal use of the University email system is permitted as a privilege, not a right. Such personal use must be **non-commercial and lawful**. For example, it's acceptable to occasionally email family or handle personal matters, but using the SMVDU email for running an outside business, political campaigning, or large personal file storage is not allowed. Users should understand that personal emails sent through University accounts may still be subject to monitoring or disclosure under certain circumstances (e.g., legal discovery). Therefore, truly private matters should be kept to personal email outside the University system.

3. Email Content and Etiquette:

- Users shall not send emails that contain harassing, discriminatory, defamatory, or otherwise offensive content. All use must adhere to the University's code of conduct and applicable laws (e.g., no obscenity as per IT Act Section 67).
- Sending spam, chain letters, or mass unsolicited emails from University accounts is prohibited. Mass mailing to the campus community (like announcements to all students) should be done via designated channels or with appropriate approvals to avoid spamming inboxes.
- **Attachments & Links:** Exercise caution with email attachments or links, even from known senders. Users should not open attachments or click links that seem suspicious; they should report such emails as potential phishing. The IT department will deploy anti-spam and anti-phishing filters to reduce malicious emails reaching users, but vigilance is still required (as emphasized in cybersecurity training).

- **Email Signature:** It is recommended to include an official signature in emails, including the sender's name, title, and University affiliation, to clearly identify official communications.

4. Email Security and Access:

- **Credentials:** Users must guard their email passwords and never share them. Two-factor authentication for email (Google 2-Step Verification) is to be enabled by all users, significantly reducing the risk of compromised accounts.
- **Access by University:** While the University does not routinely read individuals' emails, it reserves the right to access email accounts in certain cases: for example, if required by law enforcement with proper warrants, during internal investigations of misconduct (with authorization by the Registrar/Competent Authority), or upon a user's departure to retrieve institutional data. Any such access will be logged and done with at least two authorized personnel involved, to maintain transparency.
- **Forwarding and Auto-Redirect:** Users should not auto-forward their SMVDU emails to external personal accounts without approval, as this can lead to data leaving University control and may violate privacy requirements. Official data should remain within official systems (e.g., Google Workspace which is covered by institutional agreements). Similarly, business correspondence from external emails should be forwarded or copied to official email to maintain records.
- **Account Management:** Student email accounts typically remain active during their course and for a defined period (e.g., 1 year) after graduation. Faculty/staff accounts are disabled upon separation from the University (with possible grace period or auto-reply window) and archived as needed. The IT department will deactivate or delete accounts in a timely manner once a user is no longer authorized, to prevent misuse.

5. Communication Tools (Chat, Video Conferencing, etc.): The University's Google Workspace includes services like Google Chat, Meet, and Drive. Usage of these is similarly governed:

- Chats and online meetings should uphold professional etiquette. Do not share confidential information in chats unless it's a secure authorized group.
- Recording of meetings or classes requires consent of participants or prior notification, especially if those recordings will be shared. All recordings of lectures that include student participation must adhere to privacy norms (e.g., if published, student faces/names should be removed unless they consent).
- Official announcements or instructions should be over email or official portals, not solely via transient chat messages, to ensure proper documentation and delivery.

6. Email Retention and Backup: Recognizing the importance of email communications:

- The University will implement an **email retention/archiving solution** for institutional memory and compliance. All incoming/outgoing emails on the official system may be archived for a specified duration (e.g., 1 year or as required) to meet regulatory or legal needs. This also helps retrieve critical data if needed after deletion from individual mailboxes.
- Users should not rely on their individual mailbox as the sole store of critical documents – anything important should also be saved in appropriate University document repositories or backups.
- The IT department performs regular backups of Google Workspace data or ensures retention policies are in place (Google's Vault or backup tools) such that accidental deletions can be recovered within a reasonable time.

7. Internet and Social Media Use: Though primarily about email, this policy also touches on general electronic communication:

- Use of messaging platforms or social media on University network should be responsible. If identifying as a member of SMVDU online (in email signature, social profile, etc.), ensure that opinions are clearly personal if not official.
- University logos or branding in communications should be used as per official guidelines; any mass external communication representing the University should be approved by the Public Relations or relevant office.

8. Prohibited Communications: The University strictly forbids using its IT communications for:

- **Political or Religious Promotion:** Using University email or networks to forward partisan political propaganda, or to proselytize for any religious cause, is not allowed (except discussion of such topics in academic contexts). Uploading or circulating content that could inflame religious or political sentiments using University resources is prohibited.
- **Harassment or Hate Speech:** Any communication that harasses, bullies, or attacks a person/group on the basis of race, religion, gender, etc., is against both policy and law.
- **Illegal Activities:** This includes phishing, fraud, threats, or any form of cybercrime committed via University IT facilities.
- **Privacy Violations:** Do not email or share personal data of others (like lists of students' personal information) without authorization. The DPDP Act's consent requirements extend to electronic sharing as well.

Through this Email and Communication Policy, SMVDU aims to facilitate open, productive communication in support of its mission, while safeguarding the integrity of information exchange and the reputation of the University.

Academic and Research Technology Use

SMVDU embraces digital technologies to enhance teaching, learning, and research, in line with NEP 2020 and UGC's vision for technology-enabled education. This section sets policy for academic IT resources, e-learning platforms, and research computing:

1. Learning Management System (LMS) and E-Learning:

- The University will support official **Learning Management Systems** for courses (such as Moodle or other platforms, and also leverage national platforms like SWAYAM). Faculty are encouraged to use the official LMS for sharing course materials, assignments, and conducting online assessments. The IT department will ensure the LMS is integrated with student enrollment data (e.g., via Samarth ERP) for seamless access.
- **Access and Usage:** All students and instructors will be provisioned accounts on the LMS. Usage of the LMS must conform to copyright laws and academic integrity. Uploading of course content should respect intellectual property – either the instructor's own material, licensed content, or open educational resources (OER). Sharing of licensed textbooks or pirated content via LMS is not allowed.
- **Online Classes & Tools:** When conducting online classes or webinars (e.g., via Google Meet or other tools), faculty should schedule and communicate through official channels. Recording of classes must heed privacy (notify students in advance). The University may provide a licensed video conferencing platform for large classes or events if needed.
- **E-Content Development:** In alignment with NEP 2020's push for digital content creation, faculty are encouraged to develop e-content (lecture videos, quizzes, simulations). The University will clarify intellectual property rights of such content in a separate IPR policy – generally, content developed as part of teaching may remain with the University or be shared under open licenses for wider benefit, with due credit to creators.
- **MOOCs and External Platforms:** The University supports use of external platforms (Coursera, edX, NPTEL etc.) for augmenting learning. If students take MOOCs for credit (through ABC framework), the policy for credit transfer as per Academic Council guidelines applies. Technology use for proctoring online exams (if needed) will be employed with care to privacy – any proctoring software must be approved by the University and used only when in-person exams are not feasible.

- **Accessibility:** Digital learning tools should accommodate students with disabilities (screen reader compatibility, captions in videos, etc.), fulfilling the University's commitment to inclusive education per RPWD Act. Faculty should ensure their online materials are accessible or provide alternative formats on request.

2. Academic Integrity and Plagiarism:

- The University deploys plagiarism detection software (such as Turnitin, Urkund, or similar) for checking theses, dissertations, and sometimes assignments. Students and researchers must comply with guidelines on academic honesty. Submitting work through these tools is mandatory when required by the instructor or University rules. High similarity indices will be scrutinized under the plagiarism policy (as per UGC regulations on Academic Integrity).
- Any attempt to **misuse technology to gain unfair academic advantage** (hacking into grading systems, altering files, using communication devices to cheat in exams, etc.) is strictly prohibited and will face academic penalties in addition to IT policy sanctions.
- Digital assessments (online quizzes/exams) should be run on secure platforms with proper authentication. If remote proctoring is used, it must be limited to the extent necessary and in compliance with privacy norms – ideally leveraging AI proctoring tools that are vetted and with human review for flagged incidents, rather than intrusive monitoring.

3. Research Computing Facilities:

- SMVDU is building capabilities for research computing, including **High-Performance Computing (HPC)** clusters, specialized labs for AI/ML, IoT, etc. Usage of any central computing facilities (like an HPC cluster, if available) requires prior authorization from the research committee or IT department. Researchers needing such resources must apply, indicating their requirements. Fair scheduling of compute time or GPU usage will be maintained so that multiple projects can be served.
- **Data Management in Research:** Researchers are expected to follow data management best practices, especially for funded projects. Research data should be stored securely (on University research data storage or secure cloud) with backups. Any sensitive research data (e.g., involving human subjects, or national security-related) must have controlled access. Ethical clearances and data protection measures should be in place for research involving personal data.
- The University encourages depositing of published research outputs in **Shodhganga** (for theses) and using **IRINS** (Indian Research Information Network System) for profiling publications. Integration with such platforms

means faculty and research scholars should provide necessary information to the library/research cell. The IT policy supports this by ensuring the required metadata and possibly APIs are facilitated between our systems and these national repositories.

- **UGC-CARE Journals and Digital Libraries:** Access to digital libraries, journal databases, and e-resources is provided via the campus network and remote access tools. Users must adhere to license terms of these resources (e.g., do not download entire issues of journals – which can trigger publisher blocks). The library and IT will monitor for excessive or automated downloads that violate fair use policies of content providers.

4. Specialized Software and Labs:

- Different academic programs may use specialized software (e.g., MATLAB, AutoCAD, SPSS). The University maintains licenses for key software, and these are installed in labs or made available via remote access if possible. Students and faculty should use these legally provided copies and not install personal pirated versions.
- **Virtual Labs:** In coordination with national initiatives, virtual lab resources (online lab simulations and remote instrumentation) will be made available especially for disciplines where physical lab access is limited. Students are encouraged to utilize these for enhanced practical learning.
- **Internet Use in Academics:** Internet access in labs and libraries is for academic use. Sites and services that are clearly unrelated to academics may be blocked in those areas to maintain bandwidth for educational use. However, academic freedom is respected – legitimate academic use of social media or other tools (for study of those phenomena, for instance) will not be unreasonably constrained.

5. Collaboration and Communication:

- Faculty and students are urged to use the University-provided collaboration tools (Google Classroom, Drive, etc.) for academic collaboration. These tools are within our administrative control and more secure. If external tools (e.g., WhatsApp groups, Slack, etc.) are used for class discussions or project coordination, an effort should be made to eventually archive important information back to official systems for record-keeping.
- Group email lists, discussion forums, or student portals should be used responsibly and moderated as needed to prevent abuse (like trolling or sharing pirated notes).

By setting these policies, SMVDU aims to foster an environment where technology is leveraged to its fullest for academic excellence, while ensuring compliance with academic standards, digital ethics, and resource fairness.

Cloud and SaaS Usage

In pursuit of modernizing IT services, SMVDU uses cloud computing and Software-as-a-Service (SaaS) solutions for various needs (email, ERP, storage, etc.). This section outlines how cloud services are selected, used, and managed securely:

1. Cloud Strategy Alignment: The University's adoption of cloud services aligns with the Government of India's Cloud First approach under **MeghRaj (GI Cloud)**. The goal is to improve e-service delivery and optimize costs by leveraging cloud infrastructure, without compromising data sovereignty or security. Key guidelines include:

- **Data Residency:** Prefer cloud providers that host data on servers located in India for sensitive or personal data, to ease compliance with DPDP Act and government norms. If using global cloud providers (like Google), ensure the contracts or settings allow data to be restricted or mirrored in India where possible.
- **MeitY Empanelment:** When choosing cloud services for governmental or university data, priority is given to those empanelled by MeitY or meeting similar criteria (e.g., AWS, Azure, etc., if they are on the empanelled list or certified for government use).
- **Hybrid Approach:** Some services may remain on-premises (like certain databases or applications that require low latency or high control), while others move to cloud. A careful assessment will determine the best environment for each application.

2. SaaS Applications: SMVDU utilizes several SaaS platforms:

- **Samarth ERP:** A cloud-based (or centrally hosted) ERP system for academic and administrative management (covering admissions, student records, HR, finance, etc.). Integration of Samarth ERP with other systems is a priority – for example, single sign-on with Google accounts, data feed to library systems, etc., to avoid siloed data.
- **Google Workspace (G Suite):** Provides email, calendar, Drive, Docs, etc. This is a SaaS platform under a contract that provides enterprise features and enhanced security to the University. The Google Workspace admin console is managed by the IT department to enforce security policies (like 2FA, data loss prevention for Drive, etc.). Google's services comply with major security standards and are configured to meet our policy requirements for retention and auditing.
- **Learning Management (if cloud-hosted):** If our LMS is cloud-hosted (e.g., MoodleCloud or another service), similar security measures and data protections must be in place.

- **Other SaaS**: Systems like online library portals, placement cell software, accounting systems, or survey tools may be used. Each such tool must be vetted by IT for compliance with privacy and security standards before institutional adoption.

For any SaaS, the University will maintain admin control and ownership of the data. Users should use their official credentials to access these, enabling centralized management and revoke access when needed.

3. Cloud Security and Governance:

- **Access Control:** Administrator privileges for cloud services (like the Google Workspace super admin, or cloud server consoles) are limited to designated IT personnel. Activities of admins on cloud dashboards should be logged (many services provide admin audit logs) and periodically reviewed to ensure no unauthorized changes.
- **Identity and Provisioning:** Wherever possible, integrate cloud services with a central identity provider. For instance, use the Google account (or a future central SSO system) to login to multiple services (via SAML or OAuth) – this allows centralized control (if an account is disabled, access to all linked services is cut off). Role-Based Access Control principles apply on cloud as well – e.g., a faculty role might allow creating cloud VMs for research, but a student role might not.
- **Data Protection on Cloud:** Ensure that data stored or processed in cloud services is protected similar to on-premise:
    - Use encryption options offered by cloud providers (encryption at rest and in transit). Manage encryption keys if applicable or trust provider's managed keys for convenience but with awareness.
    - Configure proper backups for cloud data. Although cloud is robust, accidental deletions can occur; either utilize built-in backup features or third-party backup services for critical SaaS data (like email, Drive, ERP database).
    - Regularly review who has access to shared cloud resources (like shared drives, cloud storage buckets) to avoid open exposures. Remove or adjust permissions as roles change.
- **Vendor Management:** All cloud service providers must sign acceptable terms with the University. Key points include confidentiality of our data, breach notification commitments, compliance with Indian laws (for example, complying with law enforcement requests routed properly, etc.), and portability of data if we choose to leave the service. The IT department in coordination with the legal cell will review contracts or Terms of Service of major cloud vendors to ensure they meet our requirements.

- **MeghRaj Compliance:** If using GI Cloud infrastructure (like NIC's cloud), follow any guidelines they provide for government data classification and deployment. If using public clouds (AWS/Azure), avoid using regions outside India for sensitive workloads. Leverage any Government Community Cloud offerings if available for educational institutions, which might have pre-vetted environments.

4. Cloud Application Development & Deployment:

- If the University develops its own applications and hosts them on cloud VMs or platforms, secure development life cycle must be followed. Credentials to cloud (API keys, etc.) must be stored securely, not hard-coded or left in public repositories.
- Do not spin up cloud servers or services using University name without IT department awareness. Shadow IT (unapproved apps using University data on cloud) can introduce risks. All departments should route new cloud app requests through IT governance processes for evaluation.
- Maintain an **inventory of cloud assets** similar to physical assets. E.g., list all cloud servers, storage buckets, major SaaS subscriptions, along with their purpose, data stored, and responsible owner.

5. Usage Guidelines for Users:

- Users leveraging cloud resources (like uploading files to Google Drive or using Office 365 online, etc.) should follow good practices: label sensitive documents and if sharing, only share with intended recipients (avoid public links for internal documents). Google Drive's DLP may flag if someone tries to share personal data publicly – such flags should be heeded.
- Avoid duplicating data across multiple cloud platforms unnecessarily (to reduce sprawl and inconsistency). Use the designated official platform for a given purpose (e.g., OneDrive or Dropbox should not be used for work files if Google Drive is the standard, unless officially allowed for a specific reason).
- **Cloud Etiquette and Cost Awareness:** While many services in education plans are unlimited or fixed cost, some cloud usage can incur cost (for instance, sending bulk SMS via a cloud service, or using Google Maps API, etc.). Ensure budgetary approval for any usage that might generate cloud fees. Users given access to such services must stay within allocated quotas or budget.

The University's cloud and SaaS usage aims to be agile and innovative, providing state-of-the-art tools to the community, but always with a strong governance umbrella to protect data and ensure compliance with national initiatives and legal obligations.

User Access Management and Role-Based Controls

Managing user identities and their access rights is central to IT security. This section describes how SMVDU handles account provisioning, role-based access control (RBAC), and lifecycle events (like onboarding or leaving):

1. User Account Provisioning:

- **New Students:** When students enroll, accounts will be created for all necessary systems – an email/Google account, Samarth ERP login, LMS access, library access, etc. The Samarth ERP (or admission system) is the source of truth for student data and will trigger IT account creation. Student accounts will be placed in appropriate groups (e.g., by batch, department) to ease communication and access control.
- **New Employees:** Upon joining, faculty and staff will get accounts similarly (email, ERP HR module, etc.). The HR or Establishment section will inform IT of new hires so that accounts are ready by the start date. Multi-factor authentication and initial training in IT policy will be part of onboarding.
- **Third-Party / Guest Accounts:** Sometimes external collaborators, visiting faculty, or interns need limited-period access to certain systems. Such accounts may be created with an expiration date and least privileges required. A University sponsor (permanent staff) must vouch for and oversee any external account usage.

2. Role-Based Access Control (RBAC):

- The University will define roles (and groups) in IT systems corresponding to real-world roles. For example: Student, Faculty, Staff (with sub-roles like Accounts Staff, Librarian, etc.), Research Scholar, Alumni, Administrator. Each role/group has predetermined access rights. *E.g.*, “Faculty” group might have access to create course content on LMS, view students in their classes, whereas “Student” group can view own grades, submit assignments, etc. Similarly, an “Accounts Staff” role might allow access to financial systems but not student grades, etc.
- These role groupings are implemented in Google Workspace (Groups for email lists and Drive permissions), in Samarth ERP (user roles for different modules), and other services. The IT admin will coordinate with functional departments to ensure roles are up-to-date.
- **Principle of Least Privilege:** Users get the role that fits their official function and no more. Elevated access (like system admin privileges, or database access) is granted only to those who require it for their job and approved by the IT Head. Any temporary elevation (for troubleshooting, etc.) should be time-bound and logged.

3. Onboarding and Offboarding Processes:

- **Onboarding:** New users will receive a briefing (or documentation) on acceptable IT use and security practices as they are given access. They must sign an acknowledgment of the IT Policy (for employees, part of joining formalities; for students, part of admission confirmation or orientation).
- **Offboarding (Exit Process):**
    - For **students graduating or leaving**: Their accounts will be suspended a certain period after course completion (e.g., 6 months after graduation). During this grace period, students should backup any personal data from email or drives. After the grace, accounts may be deleted or converted to alumni status (with limited services). Any University-owned data (like project reports) should be archived by the department before deletion.
    - For **employees leaving**: Access is removed on the last working day. Email accounts of faculty/staff may be kept alive for a short period (e.g., 1 month) with out-of-office replies, then archived and disabled. HR and IT coordinate on this. All assets (laptops, ID cards, etc.) must be returned and any locally stored University data moved to a secure location. Accounts on internal systems (ERP, VPN, etc.) are promptly deactivated. The principle is to close avenues that could be misused, while preserving institutional data (emails and files are archived).
    - **Transfer of Ownership:** If a person responsible for some digital resources leaves (say a Google Drive folder owner), IT will transfer those to a new owner or a generic departmental account to maintain continuity.
- **Periodic User Access Reviews:** At least annually, the IT department in collaboration with department heads will review user lists in critical systems to ensure that no active account belongs to someone who has left or changed role. Also, check that privileges match current roles (sometimes people change positions internally and access needs adjustment). This audit helps maintain a clean access control posture.

4. Privileged Access Management:

- Accounts with administrative privileges (root, administrator, database admin, etc.) shall be limited in number. Each such account should ideally be assigned to an individual (no generic “admin” logins, or if they exist, use individual credentials via a vault). Admins should use a separate non-privileged account for routine work and only invoke privileged account when necessary (to reduce risk).
- Use of a **Privileged Access Management (PAM)** tool or at least procedures (like logging commands run as root) is recommended. All actions by privileged

users on servers or critical network devices must be traceable. For instance, enabling command history logging, and requiring ticket references for major changes.

- Default accounts (like “administrator” on Windows, “pi” on Raspberry Pis, etc.) must be renamed or disabled if not needed, to reduce known targets.

5. Multi-factor Authentication & Identity Federation:

- As mentioned earlier, 2FA is mandatory for privileged and highly sensitive accounts, and encouraged widely. The University will implement technologies to enforce 2FA (like Google 2-Step for email, VPN OTP tokens for remote access).
- The University might implement an Identity Federation or Single Sign-On system so that one set of credentials (with MFA) secures access to multiple services (reducing password fatigue and phishing risk). E.g., logging into Samarth ERP via institutional Google account SSO.
- Password resets and account recovery: The IT support will verify identity (through institutional ID, security questions, or alternate email/phone if set up) before resetting passwords to prevent social engineering exploits.

6. Access for Special Cases:

- **Shared Devices/Classroom PCs:** Some lab computers or classroom podium PCs may have a generic login for ease of use. Those should have minimal access (local access only, not logged into personal accounts by default) and be locked down (no installation rights, etc.). Users should avoid performing sensitive logins on such shared machines or remember to logout.
- **Service Accounts:** Certain applications or integrations might use non-human service accounts (for backups, application integration). Those accounts should have only the necessary permissions and their credentials stored securely. They must not be used by people to login interactively.
- **Emergency Access:** Procedures should exist for emergency access if an admin is unavailable (like break-glass accounts sealed and accessible to a higher authority under dual control).

7. Accountability: Every user is accountable for activities performed with their account. Do not share accounts or leave logged-in sessions unattended. If you suspect your account is compromised, report and change credentials immediately. Using someone else’s account or misrepresenting identity is considered a serious violation.

By meticulously managing user access throughout its lifecycle and aligning privileges with roles, SMVDU ensures a secure and efficient environment where users have appropriate access to perform their duties – no more, no less.

IT Support and Escalation Matrix

The University provides IT support to ensure that users can effectively use technology resources and that issues are resolved in a timely manner. This section describes how to obtain support and how technical issues or requests are escalated:

1. IT Helpdesk and Support Channels:

- A centralized **IT Helpdesk** is available for all users to report IT issues or requests. The primary mode is through the **Samarth ERP Portal's Helpdesk module** or a dedicated support email/portal designated by the IT department. Users can log tickets for problems (network issues, email problems, hardware faults, software installation requests, etc.) or requests (new software, access requests, etc.).
- Additionally, urgent issues can be reported via phone to the Network/IT Centre during business hours. The contact information for IT support (phone number, email, portal link) will be published on the University intranet/website and communicated to all.
- The helpdesk system will track each ticket with a unique ID, the date/time reported, and the status. Users should use this system to ensure issues aren't lost and to allow proper tracking and accountability.

2. Service Level Agreements (SLAs):

- The IT department will operate with target SLAs for response and resolution times depending on the severity of the issue:
    - **Critical issues** (e.g., network down campus-wide, major server outage, security breach): Response within 1 hour, work continuous until resolved or workaround provided. Escalation to top priority.
    - **High priority** (e.g., classroom projector failure during exams, key application down for a department): Response within 4 hours, resolution or workaround within 1 business day.
    - **Medium priority** (e.g., individual PC issues, software help): Response within 1 business day, resolve in 3 days.
    - **Low priority** (minor inconveniences, general queries): Best effort, usually within 5 business days.
- These are guidelines; actual resolution may vary, but setting expectations helps users and IT manage workloads. The IT helpdesk tool will reflect these priorities.

3. Support Scope:

- **Hardware Support:** The IT team (or designated vendor for AMC) will support University-owned hardware like office PCs, lab computers, servers, networking gear, printers, etc. For personally-owned devices, support may be limited to network connectivity help or advising (users are responsible for their maintenance, but IT can provide guidance).
- **Software Support:** Assistance will be provided for standard software (OS issues, university-licensed software, email setup, etc.). For specialized software used by certain departments, there may be specific support contacts (like a lab assistant or vendor support) – IT helpdesk will coordinate if needed.
- **Account/Access Issues:** Password resets, account lockouts, permission issues are handled promptly given their impact on user productivity (with proper identity verification as mentioned earlier).

4. Escalation Matrix:

If an issue is not resolved or is particularly complex, an escalation path is defined:

- Level 1: Helpdesk Technician / Junior Engineer – initial troubleshooting and resolution. If it cannot be solved at this level within the expected time, escalate to:
- Level 2: Senior IT Engineer or System Administrator – handles more complex problems, server-side issues, network configuration, etc. They may remotely connect or come on-site for detailed fix.
- Level 3: IT Manager / Director of IT – If issue remains unresolved or requires managerial decisions (like purchasing replacement hardware, invoking DR plan, etc.), it goes to the IT head. Also, if multiple users are affected or SLA is breached, IT head is alerted.
- Level 4: IT Steering Committee / Higher Administration – Only for extreme cases such as significant outages or policy-related issues. For example, if a critical system is down for long or a major project decision is needed, the matter can be escalated to the Registrar or relevant committee for urgent intervention (like allocating emergency funds, hiring external experts, etc.).
- This escalation is also in terms of communication: users can ask for their ticket to be escalated if they feel it's not being addressed properly. There's an appeal route: e.g., contact the IT Manager if the Helpdesk is non-responsive.

The **Samarth portal** or helpdesk system might automate some escalation: e.g., if a ticket is open beyond X hours without update, it automatically notifies the next level supervisor.

5. Incident Handling vs. Request Fulfillment:

- There's a distinction between incidents (things broken that need fixing) and service requests (asking for something new). The process for both is through

the helpdesk, but requests might require approvals (for instance, requesting new software or higher access might need supervisor approval or budget). The helpdesk workflow will incorporate any necessary approvals electronically.

- For security incidents or data privacy issues, users can still use the helpdesk but those will be **routed directly to the IT Security team and DPO** rather than the normal queue, due to sensitivity (and handled under the Incident Response procedures discussed earlier).

6. Communication and Feedback:

- The IT support team will keep the user informed of progress: acknowledge the ticket, update when in progress, notify upon resolution with what was done.
- Users should provide feedback on support experience. Feedback mechanisms (a short survey or rating on ticket closure) will help improve the service. Repeated patterns of issues will be analyzed to address root causes (problem management).
- If a user has a complaint about how their IT issue was handled, they can escalate it to the Director of IT or ultimately to the Registrar's office. The University encourages resolving such issues amicably and using them to refine support processes.

By establishing a clear helpdesk system and escalation matrix, SMVDU ensures that IT-related problems are addressed efficiently and transparently, minimizing downtime and user frustration, and continuously improving service quality.

Monitoring, Logging, and Auditing

To maintain the security and efficiency of its IT environment, SMVDU will engage in prudent monitoring and auditing of systems and usage. These activities are conducted in a transparent and lawful manner, primarily to detect problems, ensure compliance, and plan capacity. Key points include:

1. System and Network Monitoring:

- The University employs monitoring tools to supervise network traffic and critical system performance. This includes real-time alerts for outages, unusual spikes in traffic, or security events (as part of the SIEM mentioned earlier). For example, the network team monitors link utilization to identify congestion or potential abuses (like torrents).
- **Content Filtering Logs:** The Sophos firewall and proxy servers log website access attempts (URLs visited, blocked content categories) as part of maintaining a secure environment. These logs are reviewed if needed to investigate security incidents or policy violations. Routine web filtering is mainly automated, but administrators can generate reports of top sites, bandwidth

users, etc., to inform management decisions (like needing more bandwidth or adjusting filters).

- **System Logs:** Servers (authentication logs, application logs) and endpoints produce logs. All critical systems are configured to keep logs of user login attempts (successful and failed), configuration changes, and access to important data. In line with CERT-In directives, **logs of ICT systems are retained for at least 180 days** within Indian jurisdiction. In practice, the University aims to store key logs for even longer (e.g., one year) if storage permits, especially for systems like ERP and firewall logs.
- A **time synchronization service (NTP)** will ensure all logs have accurate timestamps.

2. Privacy and Ethical Considerations in Monitoring:

- The University does **not engage in continuous surveillance of individual users** without cause. Monitoring is generally at the systems level (e.g., overall network flows, server access logs) and not targeting personal content. However, users should be aware (as noted in Data Privacy section) that their activities on University IT resources are logged and can be reviewed if a security alert or investigation warrants it.
- Any inspection of a specific user's digital activities (such as reading logins or email metadata) requires authorization from senior officials (Registrar/DPO) and will be done by a limited number of personnel. The purpose would only be to confirm or investigate suspected violations or threats.
- The University will comply with any lawful interception or monitoring requests from government agencies, as empowered by the IT Act Section 69 or others, but such compliance will be done formally and documented (e.g., if law enforcement needs logs for an inquiry, the request and response are recorded).

3. Internal and External Audits:

- **Internal Audits:** The IT department will perform regular internal audits of systems and processes, at least annually. This includes security configuration audits, permission audits (ensuring users have correct access), software license compliance audits, and policy compliance spot-checks (like checking if departments are following data classification, etc.). Findings will be reported to the IT Steering Committee and action plans made for any deficiencies.
- **External Audits:** The University may engage external auditors or experts periodically (e.g., every 2 years or as required by accreditation bodies) to audit IT security and compliance. An external vulnerability assessment and penetration test of critical infrastructure is recommended annually. Financial audits might also cover IT assets and software licensing.

- **Compliance Audits:** If required by specific laws (e.g., if designated as a Significant Data Fiduciary under DPDP Act in future, which would require data audits), those will be carried out. Also, audits aligned with ISO standards or NAAC/NBA accreditation requirements for IT are performed as needed.

4. Monitoring of IT Services Performance:

- Aside from security, monitoring is used for performance and capacity planning. For instance, track uptime of the ERP system, response times, database loads, etc. Key metrics (KPIs) might include network uptime percentage, average time to resolve tickets, number of security incidents per quarter, etc. These metrics will be reviewed by IT management to gauge if objectives are met and where improvements are needed.
- The University targets high availability. If any critical service has frequent downtime beyond acceptable limits, an investigation will determine if upgrades or changes are required (like adding redundancy, increasing bandwidth, etc.).

5. Logging and Audit Trails:

- **User Activity Logs:** Applications like ERP and LMS maintain audit trails of important actions (such as who edited a grade, who accessed a sensitive record, etc.). These logs help in accountability. For example, Samarth ERP should log when an admin views or changes personal data fields, to prevent unauthorized snooping – and these logs can be reviewed by the DPO if a privacy complaint arises.
- **Administrative Actions:** All changes to network configurations, firewall rules, creation/deletion of user accounts, etc., should be logged with details of which administrator performed them. Version control or change management systems should be used for tracking configuration changes in code or infrastructure. This provides traceability and ability to roll back if a change caused issues.
- Logs will be protected from tampering – ideally, centralized logging to a secure server is implemented so that if a particular system is compromised, its logs are already stored safely.

6. Centralized Logging (SIEM):

- As part of improving threat detection, a Security Information and Event Management system correlates events from various logs to spot patterns (like multiple failed logins across different servers might indicate a targeted attack). The SIEM or log management solution will generate alerts for the security team to investigate in near real-time.
- Over time, machine learning or advanced analytics might be applied to detect anomalies (user logging in at odd hours or from different locations, etc., which might indicate account compromise).

- Centralized logging via the SIEM shall correlate events across Sophos Firewall, servers, ERP/LMS, and endpoint agents to enable near-real-time detection and response, with mandatory ≥180-day log retention within India as per CERT-In.

7. Data Analytics and Continuous Improvement:

- The IT department will analyze support tickets, usage logs, etc., to identify where training may be needed (e.g., if many people fall for phishing attempts, do more awareness; if certain software often crashes, consider alternatives).
- **Continuous Improvement Loop:** Monitoring findings -> Audit reports -> Management review -> Policy or process changes. The IT policy itself will be updated if audits reveal any gap or a new risk to address (see Review section).

All monitoring and audit activities are done with the intent to protect the University's IT environment and its users. They will be conducted professionally, confidentially, and results used constructively to enhance systems and not to unjustly infringe on individual privacy. The existence of these logs and audits also serves as a deterrent against policy violations, since misuse can be traced.

Training and Awareness

Technology is only as secure and effective as the people who use it. SMVDU therefore places strong emphasis on IT training and awareness to cultivate a knowledgeable user community:

1. Orientation and Onboarding Training:

- All new students and employees will receive an introduction to the IT facilities and policies of the University. For students, this may be part of the orientation program – covering how to use email, LMS, library e-resources, and highlighting key "dos and don'ts" of the IT Policy. For employees, an IT briefing is part of joining formalities. New faculty, for example, would be briefed on using Samarth ERP for grading, using official email, data privacy responsibilities, etc.
- A concise IT User Handbook or summary of this policy will be provided, covering critical points like proper email use, password rules, incident reporting, and support contacts.

2. Cybersecurity Awareness Campaigns:

- Regular awareness initiatives will be conducted to keep the community alert to cyber threats. This includes:
    - **Phishing Drills:** The IT Security team may conduct simulated phishing email campaigns to gauge vigilance. Users who click on fake phishing links will be redirected to an educational page explaining the red flags

they missed. The aim is not to punish but to educate users in a practical way.

- **Workshops and Webinars:** At least each semester, sessions on topics like "Protecting Your Data," "Secure Use of Social Media," "Avoiding Malware," etc., will be offered. Professionals (possibly including law enforcement cyber cell officers or industry experts) might be invited to speak. The UGC has urged institutions to hold such workshops using its cybersecurity handbook, and SMVDU will integrate those guidelines (e.g., covering strong passwords, phishing recognition, safe browsing) in these sessions.
- **Cybersecurity Handbook Distribution:** The UGC's "Cybersecurity for Higher Education Institutions" handbook (or University's own material) will be made accessible to all stakeholders as a reference. Key points from it (like common cyber threats and responses) will be periodically highlighted via emails or posters.
- **Posters/Infographics:** Visible reminders placed on notice boards and login screens about security best practices – e.g., "Think before you click," "Keep your password secret," "Report incidents promptly," etc.

3. Data Privacy and DPDP Act Training:

- Specialized training, especially for staff handling personal data (admissions, exam section, HR), on the requirements of the DPDP Act 2023 is essential. This covers how to collect consent, how to handle data access requests, and what to do in case of a potential breach. The DPO will organize annual refresher training for data-handling units to ensure they follow privacy by design.
- Students and faculty should also be aware of data privacy principles, as they might be data principals or even data custodians in research. The University may incorporate a brief module on digital privacy and ethics in relevant coursework or as a seminar.

4. IT Skill Development:

- Beyond security, the University will offer training for effective use of IT resources:
  - **Productivity Tools:** Sessions on advanced features of Google Workspace, data analysis tools, or presentation software for both students and staff.
  - **Academic Tech Training:** Faculty might need training on using the LMS, creating online quizzes, or using plagiarism checkers. Similarly, librarians can train researchers on using digital libraries or reference management tools.

- **Specialized Software:** Departments, with IT support, should ensure users are trained on any specialized academic software (e.g., CAD tools for engineering, statistical software for management studies). This could involve vendor demonstrations or peer training.
- **ERP Training:** Since Samarth ERP will be used by many (faculty entering grades, students checking info, staff managing processes), periodic training and updated user manuals will be provided whenever modules are changed or new features added.

5. Mandatory Compliance Training:

- The University may mandate that all employees complete an annual IT security awareness training (delivered online) and pass a quick quiz. This ensures everyone is up-to-date on policies and threats. Non-compliance could result in reminders or even account restrictions until training is done, given how critical user awareness is to overall security.
- Similarly, students might have to complete a basic module on "Digital Citizenship and Security" when they join (possibly integrated into a first-year course or via the LMS with a certificate of completion).

6. Evaluation and Continuous Improvement:

- After training sessions, feedback will be collected to improve content and delivery. If awareness campaigns show persistent risky behavior (for example, many still click on phishing emails), the training approach will be rethought – maybe more interactive or targeted sessions for those who need it.
- Keep content up-to-date: Cyber threats evolve, so our training materials need to cover new scams or technology (like awareness about using AI chatbots safely, or deepfake threats, etc., as relevant).
- Ensure multi-lingual or accessible formats as needed to reach all members (the UGC handbook idea of accessibility at all levels is noted).

7. Culture of Shared Responsibility:

- The overarching message in all awareness activities is that security and good IT practice is **everyone's responsibility**. The IT department can provide tools and policies, but each user must act conscientiously – whether it's choosing a strong password, reporting a lost device immediately, or simply logging off after using a system.
- Recognize and reward departments or individuals who exhibit good practices (perhaps a "Cyber Safe Department" recognition for units with least incidents or 100% training completion, etc., to encourage friendly competition in compliance).

Through continuous training and awareness, SMVDU aims to significantly reduce human error-related incidents, enhance productivity by better IT utilization, and create an informed campus that can take full advantage of digital opportunities safely.

Integration with Samarth ERP, Google Workspace, and Sophos Firewall

SMVDU's IT ecosystem includes key platforms such as the Samarth ERP system for university management, Google Workspace for communication and collaboration, and Sophos Firewall for network security. Effective integration and use of these are crucial for a seamless and secure user experience. This section outlines policies specific to these systems:

1. Samarth ERP Integration and Use:

- **Centralized Data Management:** Samarth ERP serves as the central repository for academic and administrative data (students' academic records, faculty HR details, finance, etc.). All departments must use the ERP for relevant processes to ensure data consistency. For instance, student attendance and grades should be entered in ERP where modules exist, rather than maintaining separate local records.
- **Single Sign-On (SSO):** The University strives to integrate Samarth ERP authentication with the central SSO (currently Google Workspace accounts). Until full SSO is achieved, users will have separate ERP credentials; however, they should be synchronized with email IDs where possible and adhere to the same password policies.
- **Data Flow:** Samarth ERP will be integrated with other applications to avoid duplicate data entry. For example:
    - The LMS can fetch course enrollment data from ERP (so when students register for courses in ERP, they are auto-enrolled in LMS).
    - The library system can use student/faculty data from ERP for issuing library cards.
    - The HR module data feeds into the access control systems or ID card generation.
- **Access Control in ERP:** Users get role-based access in the ERP. A faculty member can see their course student list but not another's; a Head of Department might see departmental summary data; admin staff have permissions as per job function. The ERP admin team must regularly review these roles. Any elevated access (like viewing/editing grades outside one's class) should be granted only on written request and with approval of competent authority.

- **ERP Data Updates:** Certain self-service features are enabled – e.g., students updating their contact info, faculty applying for leave, etc. Users are expected to keep their information updated in ERP (addresses, phone numbers) for effective communication. These updates should be timely and accurate.
- **Samarth Portal for Services:** The ERP includes a portal for various services – grievances, requests for certificates, etc. Users should utilize these online services instead of paper processes when available. This not only speeds up processing but also maintains records. For example, if a student needs a Bonafide certificate, they apply in Samarth; the request flows to the concerned office, and the certificate issued is recorded.
- **Data Protection:** All personal data in ERP is protected per the Data Privacy section. ERP being a comprehensive system, the DPO will pay special attention to it – ensuring sensitive fields (like Aadhaar, exam marks, fees paid) are accessed only by those who need it and consent is captured where required (e.g., perhaps on admission form). Audit logs in ERP must be enabled to track who viewed or modified critical data.

2. Google Workspace (GW) Integration and Use:

- **Official Domain Use:** SMVDU's Google Workspace (GW) domain is the official platform for email and cloud collaboration. All official documents, spreadsheets, etc., should ideally be created and stored in this domain (Google Drive) for easy sharing within the community and retention. It's integrated with users' emails and simplifies collaboration (no need to use personal Google accounts for work).
- **Google Drive and Sharing:** Users should take advantage of Google Drive for storing University-related files. When sharing files, use domain-restricted links (accessible only to @smvdu.ac.in accounts) for internal documents instead of making them public. For external collaboration, specific people can be invited by email. This ensures control and visibility. Shared Drives (Team Drives) can be used for departments or projects so that data ownership is with the group, not an individual (which helps during staff turnover).
- **Calendar & Scheduling:** Faculty and staff should use Google Calendar on GW to schedule meetings, classes, etc. Academic calendars and resource booking (like meeting rooms) can also be managed via Calendar to improve coordination.
- **Security Features:** The IT admin will enforce or encourage use of GW security features:
    - 2-Step Verification enforcement for all users or at least admin accounts.
    - Alerts on external email tagging – GW can mark mails from outside the domain for user awareness (reducing phishing success).

  - Drive Data Loss Prevention (DLP) rules to prevent accidental sharing of sensitive info (like a rule might warn/block if someone shares a spreadsheet containing many identity numbers or such patterns outside the domain).
  - Vault: Google Vault is enabled for email and chat archival as per retention policy. Users typically will not see this, but it's part of compliance.

- **Email Groups and Communication:** GW Groups are used for mailing lists (e.g., all-students@smvdu, all-faculty@smvdu, department groups). These are managed by IT or designated owners. Only authorized senders can mail broad groups to prevent spam. Users can request creation of new groups for official purposes (like a research group discussion list) via IT. Posting rights, account validity & quotas—see Annexure-A.
- **Third-Party Apps:** Sometimes users may install third-party add-ons to Google (for productivity). IT will maintain a list of trusted add-ons; any app that asks for broad access to GW data may be blocked pending review. Users are warned to be cautious granting permissions to external apps with their GW account.
- **Account Recovery:** Users should set up account recovery options (alternate email or phone) in GW for self-service password resets. The IT admin can also force reset if needed with identity verification.

3. Sophos Firewall and Network Integration:

- **Network Admission Control:** The Sophos (or any next-gen firewall) may implement basic network access control – devices connecting to the network might be scanned or required to have an agent installed (if we use endpoint-firewall integration). For example, if Sophos endpoint protection is deployed, the firewall can check if a device has it running before granting full access. This ties into BYOD policy ensuring compliance.
- **User Authentication on Network:** Wherever feasible, network usage is tied to user identity. For Wi-Fi, 802.1x or a captive portal login with the user's ID could be used instead of a shared password. For wired networks, important locations might use NAC to register devices. The firewall can integrate with directory/SSO such that logs show which user (not just IP) accessed what, improving accountability.
- **Web and Content Filtering:** The Sophos firewall is configured with content filtering policies appropriate for a University. Academic freedom is respected, but categories like malware, pornography, extreme violence, etc., are blocked to comply with law and maintain decorum. Certain sites may be throttled (like social media during class hours on academic networks) if needed to preserve

bandwidth, though outright blocking of social sites is generally not done except on request or specific labs.

- **Application Control:** The firewall can control specific applications (like peer-to-peer file sharing protocols, torrent traffic, etc.) which are often misused. These will be generally blocked or limited on the campus network. If a legitimate academic reason exists to use such protocols (say a research project), exceptions can be made for specific systems or times.
- **Logging and Alerts:** The firewall logs, as mentioned, record network events. It also can send alerts for certain triggers (e.g., a device scanning multiple ports, possible malware beaconing out, intrusion attempts). The IT security staff will tune and monitor these alerts. In integration with SIEM, Sophos provides a significant data source for detecting intrusions.
- **VPN and Remote Access via Firewall:** If the University provides a VPN for accessing internal resources from outside, it is managed through the firewall. Only authenticated users can establish the VPN, and their access inside is limited to what's necessary (not full network if not needed). The Sophos VPN logs are monitored for unusual login attempts (failed logins might indicate someone's password is compromised).
- **Firmware Updates:** The firewall and its filter lists are kept updated by IT to defend against new threats. Sophos releases periodic updates which the network team will apply in maintenance windows. The firewall's subscriptions for antivirus, IPS, etc., will be maintained active.

4. Coordination Between Systems:

- **ERP & Firewall:** For example, if the ERP holds hostel allocations, the firewall could use that info to apply different policies (like hostel network might have different access times) – this kind of advanced integration could be explored in future.
- **Google & ERP:** If a student officially leaves (record in ERP), triggers to de-provision their Google account after grace period should be automated. Similarly, new admissions trigger Google account creation.
- **Firewall & Google:** If we detect via firewall logs that an account/email might be sending spam (unusual traffic), IT can investigate if the Google account is compromised and take action (reset password, etc.). Thus cross-referencing information from these platforms is part of incident response.

In summary, these core systems – Samarth ERP, Google Workspace, and Sophos Firewall – form the backbone of SMVDU's IT environment. The policy is to ensure they are **well-integrated, secure, and used to their full potential**. Users should be familiar with their capabilities and the rules around them, as detailed above, to both benefit from and contribute to a smooth digital campus experience.

Policy Violations and Disciplinary Procedures

All users are expected to abide by the provisions of this IT Policy. Violations of the policy undermine the security and integrity of the University's IT environment and can lead to legal liabilities or reputational damage. This section outlines what constitutes a violation and the procedures for addressing them, ensuring fairness and due process.

1. Examples of Policy Violations:

- Using someone else's credentials to access a system without authorization.
- Downloading or distributing pirated software or content using University resources.
- Knowingly propagating malware or engaging in hacking/cracking activities.
- Harassing or threatening others through University email or networks.
- Unauthorized handling of personal data (e.g., copying student records to personal devices, or leaking confidential information).
- Tampering with network equipment or connecting unauthorized devices, causing network disruption.
- Ignoring directives from IT administrators regarding security (like refusing to update a vulnerable system or not removing prohibited software).
- Repeated minor offenses (like continued storage of non-academic large files on servers, despite warnings).

2. Reporting and Detection of Violations:

- Suspected violations may be detected through monitoring (logs or alerts as described earlier) or reported by other users. For instance, if a student finds someone snooping in their account or a faculty notices exam data leak, they should report it.
- The University encourages reporting to be done via the incident reporting channels (IT helpdesk or directly to IT Security if sensitive). Good faith reports will not result in retaliation. In some cases, violations might also come to light via audits or complaints (like a copyright infringement notice from an external party).

3. Investigation Process:

- Once a potential violation is noted, the IT department (and DPO if personal data involved) will conduct a preliminary investigation. This may involve collecting evidence (log files, witness statements, copies of offending material). The user in question may be temporarily suspended from certain accesses if needed to

prevent ongoing harm (for example, disabling an account suspected of sending malware).

- Investigations will be discreet and confidential. If the matter involves a student, the Chief Warden or Dean of Student Affairs might be involved; if a staff, then HR; if faculty, possibly the Dean or a committee as appropriate. However, technical fact-finding is done by IT experts.
- The outcome of the investigation (evidence gathered) is documented. If evidence confirms a violation or is strongly suggestive, the matter moves to disciplinary action. If evidence is inconclusive or points to no fault (e.g., the anomalous activity was due to a system error), the case may be dropped with no action and the concerned user notified/cleared.

4. Disciplinary Action:

- **Minor Violations:** These might be inadvertent or first-time issues with low impact (e.g., installing an unauthorized app, or a one-time excessive personal use of bandwidth). Typically handled by a warning and guidance. The IT department can issue an email or notice to the user explaining the breach and instructing compliance. The user may have to confirm understanding of the policy. A record is kept internally of the warning.
- **Serious or Repeated Violations:** For more serious breaches or repeat offenses, formal disciplinary procedures will be invoked:
    - For **students**, the case may be referred to the **Student Disciplinary Committee** (or equivalent, as per student code of conduct). Possible sanctions include suspension of IT access (temporary or permanent), informing parents/guardians in severe cases (though this measure must be proportionate and consistent with student discipline policies), fines for damages (e.g., if physical equipment was tampered with), or in egregious cases, suspension or expulsion from the University in line with the student handbook provisions. Any financial costs due to a student's actions (like legal penalties for copyright infringement, or repair costs for deliberate damage) may be passed on to them.
    - For **faculty or staff**, violations will be handled according to employee conduct rules and HR procedures. This could involve a report to the Vice Chancellor through proper channel, and actions might range from reprimand letters, loss of certain privileges, up to termination of employment in extreme cases. The principle of progressive discipline is followed (warning -> show-cause notice -> disciplinary hearing -> action). Faculty have academic freedom, but that does not excuse legal infractions or serious policy breaches.

- For **third-party or vendor personnel**, access may be immediately revoked. Their employer will be notified, and depending on the contract, they could be barred from future engagements. If their action caused damage, the University may pursue remedies as per contract or law.

- **Legal Action:** If any violation breaks the law (such as hacking, data theft, viewing/distributing child pornography, cyber stalking, etc.), the University will involve law enforcement. The IT Act provides strict penalties for various cybercrimes, and SMVDU will not shield individuals from legal consequences. Cooperation with police/Cyber Crime Cell will be given, and any internal discipline is separate from criminal proceedings that may follow.
- **Restitution:** In cases where the University suffers financial or operational harm (e.g., a malware outbreak required spending on recovery), it may seek restitution from the responsible party. Students or staff might be asked to compensate for damages in line with University financial rules, though this is usually after an inquiry confirms willful or negligent misconduct.

5. Ensuring Fair Process:

- No user will be presumed guilty without an opportunity to explain. If you're accused of a violation, you will be informed of the allegations and evidence, and typically asked to respond (unless there's an immediate critical threat requiring instant action). For instance, a student might receive a show-cause notice detailing the alleged misconduct (with evidence like log excerpts) and can reply or appear before the committee.
- Disciplinary hearings, if held, will allow the individual to present their side. They may bring forth mitigating factors or contest the evidence. The committee will objectively evaluate before deciding.
- The disciplinary outcome will be communicated in writing. If a user believes the process was unfair or the punishment disproportionate, they have the right to appeal to a higher authority (e.g., Vice Chancellor or an Appeals Committee) as per University statutes. The IT policy defers to those general grievance/appeal mechanisms available in the University for students and staff.

6. Temporary Measures:

- During investigation, temporary actions may include: disabling an account, blocking certain network access, or seizing a device for forensic imaging (with proper authorization). These are not punishments but precautions. They will be lifted if the user is cleared or after the necessary information is obtained.
- If a user's action poses imminent threat (like an ongoing network attack), IT admins have authority to isolate that user's connection immediately in order to protect the campus.

7. Documentation and Records:

- All incidents and outcomes will be logged by the IT department. Patterns of minor violations might prompt additional training or policy clarification. Major cases and their resolutions might be summarized (with identities redacted) in reports to the IT Steering Committee for awareness and to inform policy updates.
- The confidentiality of those involved will be maintained to the extent possible. Only people who need to know (investigators, committee members, higher administration) will be informed of identities. Outcomes like expulsion or termination, if any, are handled per usual University notification processes, not broadcast via IT channels.

8. Reinstatement:

- If an IT access was suspended as a penalty (e.g., a student barred from the network for a month due to misuse), after the period, access can be restored. The user may be required to undergo some retraining or reaffirmation of compliance before reinstatement.
- In contrast, if someone was expelled or employment terminated, their access is permanently revoked.

By enforcing these disciplinary procedures, SMVDU aims to deter misuse of IT resources and provide a clear path for handling infractions. The focus is on education and prevention (hence warnings and training), but the University will act firmly when needed to maintain a secure and lawful IT environment. See Annexure-B for student penalization.

Review and Amendment Protocols

Information Technology is a fast-evolving domain, and policies must remain current with emerging technologies, threats, and regulatory changes. SMVDU commits to keeping this IT Policy up-to-date and relevant. The following outlines how the policy will be reviewed, updated, and communicated:

1. Regular Review Cycle:

- The IT Policy shall undergo a formal review **at least once every year**. The IT Steering Committee will schedule this review, typically at the end of an academic year or calendar year. During the review, the committee will evaluate if the policy is working well, any incidents or feedback suggesting changes, and consider any new laws (for example, if any rules under DPDP Act or new UGC guidelines have come out in the year).
- In addition to annual reviews, immediate reviews will be triggered by significant events:

  - Major security incident or data breach – to analyze if policy gaps contributed and need fixing.
  - Significant technology changes – e.g., adoption of a new ERP or cloud system might require new policy sections.
  - Regulatory updates – e.g., if CERT-In or MeitY issue new directives, or an amendment to IT Act/DPDP Act, etc.
  - Feedback from stakeholders – if faculty/student bodies or auditors raise concerns.
- The review process will involve consultation with key stakeholders: IT administrators, faculty representatives, student representatives (for parts that affect students), and possibly external advisors for compliance.

2. Amendment Process:

- Proposed changes to the policy will be drafted by the Director of IT or a small committee appointed for this purpose. The draft changes should highlight sections to be added, removed, or modified, with rationale.
- The draft amendments may be circulated for comment: e.g., to department heads or put on intranet for community feedback (especially if it's a major change impacting users' day-to-day usage).
- After incorporating feedback, the revised policy is submitted to the competent authority for approval. Depending on University governance, this could be the Vice Chancellor's approval, or for major policy changes, the Executive Council or a similar top body might need to ratify.
- Once approved, the new version of the policy is formally issued.

3. Version Control:

- Each iteration of the policy will be versioned (e.g., v1.0, v1.1, v2.0 etc.) and dated. A revision history at the end of the document (or a change log) will summarize what changed in each version and the approval date.
- Old versions of the policy will be archived for reference. This is important for audit trails and any cases where actions were taken under a previous policy – one can refer back to what rules were in place at that time.

4. Communication of Changes:

- Whenever the policy is updated, the University will **communicate the changes clearly to all users**. This may include:
  - An official email summarizing key changes and attaching the new policy or link to it.

  - Updates on the University website/portal where the policy is posted (ensure the latest PDF or webpage is available).
  - If changes are substantial, info sessions or webinars might be conducted to explain them and answer questions.

- Users may be required to acknowledge the updated policy (for instance, ticking a read receipt on the portal or signing an acknowledgment form especially for staff) to ensure awareness.

5. Accessibility of Policy:

- The IT Policy shall be made easily accessible to all stakeholders at all times. It will be published on the SMVDU website (policy section) for public transparency and on the intranet/student portal for current users. This allows anyone to consult it when needed.
- Efforts will be made to present the policy in a user-friendly manner, possibly including an executive summary or FAQ for quick reference. (The full formal document is binding, but summaries help understanding.)
- For visually impaired or those requiring assistive formats, the policy document will be available in accessible formats (text-based, compatible with screen readers, etc.).

6. Related Policies and Modularization:

- Over time, this comprehensive policy might be complemented by more focused sub-policies or guidelines (e.g., a separate “Data Protection Policy” elaborating DPDP compliance, or a “Bring Your Own Device Guideline”). If so, the relationship will be clearly defined (likely as appendices or referenced documents).
- The review of this master policy will include review of its sub-components. If any sub-policy needs change, that will be coordinated to keep everything consistent.

7. Governance of Policy Enforcement:

- The review will also assess how well enforcement mechanisms are working. For example, check if disciplinary processes were adequate or if perhaps an amendment is needed to address a new type of misuse.
- The IT Steering Committee during review will consider metrics: number of violations, support tickets trends, audit findings, etc., to gauge if policy adjustments can reduce issues.

8. Change Management in IT Systems:

- Though more operational, it's worth noting that any significant IT system changes will have a **change management process** (documenting, testing, approving changes) to minimize disruptions. Changes in systems often necessitate policy review too (for security or usage implications).

Conclusion: This IT Policy is a living document. By instituting a robust review and amendment protocol, SMVDU ensures that its IT governance remains agile and forward-looking. Stakeholders are encouraged to provide suggestions for improvement at any time, which will be taken into account in the formal review. The ultimate goal is a policy that continuously supports the University's mission in the digital age, balancing innovation with security and compliance.

Annexure-A

This annexure formalizes email posting rights, account deactivation/deletion timelines, and storage quotas for SMVDU users and system accounts. It should be read together with the primary Email & Communication section of the IT Policy.

S. No.	Post/ Designation	Posting Rights	Email deactivation/ suspension	Permanent Deletion of Data	Storage Quota
1	HVC/Registrar	Send to All	Not Applicable	Never	Not Applicable
2	Designation-based IDs (Dean/Directors/ HoDs/Heads)	Send to All	Not Applicable	Never	100 GB
3	Designation-based IDs (other)	Individual email-ids or smaller email groups (e.g., department groups)	Active till authority is actively using that account	Never	100 GB
4	Permanent Employees (Name-based IDs)	Individual email-ids or smaller email groups (e.g., department groups)	After 1 year of leaving the University	After 2 years of leaving the University	100 GB
5	Students	Individual email-ids	After 1 year of leaving the University	After Convocation or after 1 year of leaving the University	30 GB
6	Workshop/ Conference/ Events/ Committees etc.	Send to All	After 3 months of the event	After 6 months of the event	50 GB

Notes:

• For all the designated post email IDs, the current post holder will be responsible for any misuse of the same.

• The storage limit applies to Free Google Workspace account licenses. For paid account licenses, additional storage may be available beyond this limit.

Annexure-B

Disciplinary Penalties for Damage to Network Infrastructure (Students)

Authority & Process. Penalties are imposed **through the Dean of Students** after approval of the **Competent Authority**. Investigations follow due process; evidence may include logs, CCTV, and witness statements. Restitution covers actual repair/replacement costs plus the deterrent levy below. Appeals as per University statutes.

S.No.	Violation (examples)	Location/Scope	Responsible Group	First Offence	Repeat Offence (within 12 months)	Notes
1	Damage to network socket, faceplate, or patch cord (broken, pulled out)	Individual room	Individual	Actuals + ₹2,000 levy	Actuals + ₹4,000 levy + up to 7-day network suspension	If negligence suspected in shared room, split levy among identified users
2	Tampering with wall cabling, conduits, or AP bracket	Common area / corridor	Identified individual(s); if none, affected wing	Actuals + ₹5,000 levy (split if shared)	Actuals + ₹10,000 levy + up to 14-day network suspension (wing)	Applies where responsibility is unclear despite inquiry
3	Damage to Access Point (AP), switch, or distribution box	Common area	Identified individual(s); else affected floor	Actuals + ₹10,000 levy	Actuals + ₹20,000 levy + restitution duty (campus service)	If vandalism is proved, add community service up to 20 hours
4	Hostel-wide damage or cable cut	Hostel-wide	All hostel residents, unless culprits identified	Actuals + ₹50 per resident levy	Actuals + ₹100 per resident levy + up to	Throttling is corrective, not

S.No.	Violation (examples)	Location/Scope	Responsible Group	First Offence	Repeat Offence (within 12 months)	Notes
5	Installing unauthorized routers/switches; rogue AP; bypassing firewall	Any	Individual	₹3,000 levy + device confiscation (returned at end of term); up to 7-day suspension	₹6,000 levy + 14-day suspension	Separate action applies if academic integrity was affected
6	Intentional damage/sabotage (proved)	Any	Individual (and accomplices)	Actuals + ₹25,000 levy + up to 30-day suspension	Actuals + ₹50,000 levy + recommendation for disciplinary board action	May escalate to police complaint if warranted

General rules

- “Actuals” = verified repair/replacement cost billed to University.
- Levies are indicative ceilings; Dean of Students may reduce for minor/accidental cases or increase (max +50%) for aggravating factors (repeat, collusion, exam disruption), with reasons recorded.
- Collective penalties apply only when responsible individuals cannot be identified after reasonable inquiry.
- Payment windows and community-service assignments are communicated with receipts and completion records.
- Nothing in this annexure precludes separate proceedings for misconduct under other University rules or law.