VIDYASHILP UNIVERSITY

Draft IT Policy

In today's digital-first environment, Information and Communication Technology (ICT) forms the foundation of academic, research, administrative, and communication activities at Vidyashilp University. The University relies extensively on digital platforms, cloud services, communication networks, enterprise applications, and computing systems to support learning, teaching, governance, and institutional operations.

1. Objective

This ICT Policy establishes the principles, governance framework, standards, responsibilities, and acceptable practices for the secure, reliable, ethical, and efficient use, management, operation, and protection of the University's Information and Communication Technology (ICT) resources, infrastructure, systems, applications, services, and institutional information assets.

The objectives of this policy are to:

- Ensure the secure, reliable, resilient, and efficient use of University ICT resources and services.
- Protect institutional data, systems, and digital assets.
- Promote responsible, ethical, secure, and legally compliant use of ICT resources and emerging technologies, including Artificial Intelligence (AI).
- Ensure compliance with applicable laws, cybersecurity standards, and regulatory requirements.
- Support uninterrupted academic and administrative operations.
- Support compliance with Digital Personal Data Protection (DPDP) Act, 2023.
- Establish governance mechanisms for cybersecurity, AI, cloud services, and institutional data management.

2. Scope

This policy governs all ICT resources that are owned, leased, managed, hosted, or operated by Vidyashilp University. It applies to all individuals who access or use the University's ICT systems and services, whether through the campus network or via remote access facilities.

All users of Vidyashilp University's computing, networking, and IT resources are required to comply with the rules and guidelines set forth in this policy. These provisions are designed to ensure fair, secure, and responsible use of ICT resources, while safeguarding the data, privacy, and academic or administrative work of students, faculty, and staff. The policy also outlines

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE

#125, Bettenahalli, Kundana Hobli, Chapparkallu Road, Bengaluru-562110, Karnataka
T. : +91 89511 84990 | E. : info@vidyashilp.edu.in | www.vidyashilp.edu.in

the procedures and guidelines for addressing and resolving complaints in consultation with the appropriate University authorities.

The scope of this policy includes, but is not limited to:

- Desktop computers, laptops, workstations, tablets, and mobile devices
- Servers, storage systems, backup systems, and data centers
- Wired and wireless campus networks
- Internet and intranet services
- Official email systems and collaboration platforms
- Cloud-hosted applications and services
- Enterprise applications, ERP systems, LMS platforms, and research systems
- Artificial Intelligence (AI) platforms, machine learning environments, data analytics systems, and emerging technologies used for academic, research, administrative, or operational purposes
- High Performance Computing (HPC) infrastructure, GPU-enabled systems, research computing facilities, and specialized computing environments established by the University or in collaboration with external organizations
- Printers, scanners, biometric systems, and peripheral devices
- Software, licensed applications, and digital services
- University websites, web applications, and digital portals
- Cybersecurity systems and monitoring platforms
- Institutional databases and digital records
- Examination, assessment, admissions, finance, human resources, library management, and other institutional information systems
- Personally owned devices (BYOD) that access University networks, systems, applications, or institutional data

This policy is applicable to:

- Faculty members
- Administrative and support staff
- Students and research scholars
- Contract employees and consultants
- Vendors visiting or operating in VU campus (canteen, vending, security, etc.), service providers, and implementation partners

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE

- Visiting faculty and external collaborators
- Any other individual authorized to access University ICT resources

All users mandatorily shall familiarize themselves with this policy and adhere to the guidelines, responsibilities, and procedures outlined herein.

All third-party service providers, consultants, implementation partners, vendors, and external agencies granted access to University ICT resources shall comply with the applicable provisions of this Policy and any related University procedures, standards, or agreements.

3. Laptop Usage

Vidyashilp University provides and permits the use of laptops as essential computing tools for academic, research, administrative, and institutional work. This policy defines the acceptable use, security requirements, and responsibilities associated with laptop usage within the University environment.

- Laptops owned or issued by the University must be used primarily for academic, research, and official institutional purposes.
- Personal laptops may be used on campus for academic-related activities, subject to compliance with University IT and security policies.
- All laptops used on the University network must have updated operating systems, licensed software, and active antivirus/endpoint protection software installed.
- Users must ensure that laptops are protected with strong passwords, device lock mechanisms, and encryption where supported.
- Sharing of laptop access credentials, user accounts, or unlocking devices for unauthorized persons is strictly prohibited.
- Installation of pirated, unauthorized, or unlicensed software on any laptop used within the University is strictly prohibited.
- Users must not use laptops for activities that violate University policies, including malicious activity, illegal downloads, or unauthorized commercial use.
- Access to University network resources through laptops must comply with all network, email, and security policies of the University.
- Laptops connected to the University network may be subject to security scanning, monitoring, and compliance checks.
- Users must take appropriate precautions while connecting laptops to external networks or public Wi-Fi to avoid security risks.
- Sensitive or confidential institutional data must not be stored on personal laptops unless explicitly authorized and secured through encryption and approved controls.

VIDYASHILP UNIVERSITY * BANGALORE * REGISTRAR

- Academic records, student data, examination content, research data, financial information, and other confidential institutional information shall not be stored locally on laptops unless specifically authorized and protected through approved security controls.
- Users shall not upload confidential University information, student records, employee data, examination content, research data, financial information, or other restricted institutional information to public Artificial Intelligence (AI) platforms without authorization.
- Institutional data stored on laptops must be regularly backed up to approved University storage systems or authorized cloud platforms.
- Laptops must not be left unattended in unsecured or public areas, users are responsible for their physical security at all times.
- Loss, theft, damage, compromise, or suspected unauthorized access involving laptops (whether University-owned or personally owned and used for institutional work) shall be reported to the IT Department or concerned authority within 24 hours of discovery.
- Any loss, theft, or damage to University-issued devices shall be the responsibility of the concerned user/department. Recovery or replacement costs, where applicable, shall be determined based on asset value, extent of negligence, insurance coverage, and approval by the Competent Authority.
- External storage devices connected to laptops must be scanned for malware before use.
- Users must not attempt to bypass security controls, disable antivirus software, or modify system security settings without authorization.
- The IT Department reserves the right to restrict or revoke network access for laptops that do not comply with security or policy requirements.

4. Data Storage and Protection

Vidyashilp University establishes this policy to ensure the secure storage, handling, and protection of institutional data across approved digital and physical storage systems. Thus,

- Institutional data must be classified and stored based on sensitivity (public, internal, confidential, restricted).
- University data must be stored only on approved institutional storage systems, which may include on-premises servers and approved cloud platforms.
- The University recommending the use of secure cloud storage services such as Google Drive (Google Workspace for Education) for academic, administrative, and collaborative purposes.
- Each department and the concerned responsible person must ensure that data related to their operations is accurate, properly maintained, and regularly updated at all times.

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE

- Users must store institutional data only in official University-managed accounts (e.g., University Google Workspace accounts) and not in personal cloud accounts. Confidential and Restricted information shall be encrypted during storage and transmission wherever technically feasible and supported by approved security controls. Users must ensure that shared links are not publicly exposed unless explicitly required and approved. Access to cloud storage must be protected using strong authentication, including multi-factor authentication (MFA) where available.
- Storage of sensitive, confidential, or restricted data in unauthorized cloud services or personal storage accounts is strictly prohibited.
- Users must not transfer or store sensitive data using personal email accounts, unauthorized cloud storage services, or external file-sharing platforms.
- Users shall not upload Confidential or Restricted University information, student records, employee data, examination content, research data, financial information, or other sensitive institutional information to public Artificial Intelligence (AI) platforms without authorization.
- Research data associated with sponsored projects, industry collaborations, consultancy assignments, patents, funded research, or confidential research activities shall be handled in accordance with applicable contractual, regulatory, and confidentiality requirements.
- Critical institutional data must have appropriate backup mechanisms, either through automated cloud backup services or institutional backup systems.
- The IT Department may define specific folders, shared drives, or organizational units for structured data storage and collaboration.
- The University reserves the right to monitor, audit, and manage institutional cloud storage usage to ensure compliance and security.
- Any suspected data breach, unauthorized access, or misuse of cloud storage must be reported immediately to the IT Department.

5. Data Retention

- Data must be retained only for the minimum period required for academic, administrative, legal, or operational purposes.
- The standard data retention timeline shall be as follows:
    - Operational/active data: retained as long as it is actively in use
    - Academic and administrative records: as required by regulatory guidelines

    o Research data: As per sponsor requirements, contractual obligations, regulatory requirements, or a minimum of 5 years after project completion, whichever is applicable

- Financial, audit, and statutory records: as per applicable laws
- System logs, security logs and access logs: minimum 1 year
- ERP audit logs: Minimum 1 year
- CCTV recordings: 30 days unless required for investigation or legal purposes
- Backup data: retained as per backup cycle (daily, weekly, monthly) with archival copies maintained in accordance with business continuity and disaster recovery requirements

- Retention periods may be extended where required due to legal, audit, research, or regulatory obligations.
- Data that is no longer required must be securely deleted using approved data destruction methods to prevent recovery or misuse.

6. Software Usage and Management

Vidyashilp University establishes this Policy to ensure the legal, secure, and efficient use of software across all institutional systems. The policy governs procurement, installation, usage, licensing, and maintenance of software used for academic, research, administrative, and operational purposes.

- All software used within the University must be properly licensed, legally acquired, and approved for institutional use.
- The use, installation, or distribution of pirated, cracked, or unlicensed software is strictly prohibited.
- Software procurement must follow the University's approved purchase and procurement procedures, including technical evaluation and licensing verification.
- Software procurement and deployment shall consider information security, privacy, compliance, supportability, and compatibility requirements before implementation.
- Only software approved by the IT Department or designated authority may be installed on University-owned systems and networks.
- Users must not install software on institutional systems without prior approval from the IT Department or system administrators.
- All software installations must comply with system compatibility, security standards, and institutional IT policies.
- Open-source software intended for production, research, or enterprise use shall undergo appropriate security and technical review before deployment.
- The IT Department shall maintain records of software versions, support status, license details, usage records, and installation logs, and end-of-life (EOL) information where applicable.

- Unauthorized copying, sharing, or redistribution of licensed software is strictly prohibited.
- Software must be used only for intended academic, research, or administrative purposes and must not be used for unauthorized commercial or personal gain.
- Users must not attempt to bypass license controls, activation mechanisms, or usage restrictions imposed by software vendors.
- Installation of unauthorized remote access tools, network scanning tools, hacking utilities, password-cracking tools, cryptocurrency mining software, or similar high-risk applications is strictly prohibited unless specifically approved for academic, research, or cybersecurity purposes.
- Artificial Intelligence (AI) software, plugins, browser extensions, and cloud-based AI services used for institutional purposes shall comply with University policies relating to data protection, privacy, academic integrity, and information security.
- Software that has reached End-of-Life (EOL) or is no longer supported by the vendor shall be upgraded, replaced, isolated, or retired based on risk assessment and operational requirements.
- Any software found to introduce security risks, system instability, or policy violations may be removed from University systems after consultation with the concerned user/department, with the IT Department kept informed throughout the process. In cases of critical or imminent security threats, the IT Department may take immediate action to protect University systems and notify the concerned user/department as soon as practicable.
- Periodic software compliance and license audits may be conducted to ensure adherence to licensing terms, contractual obligations, and University requirements.

7. E-Mail Usage

Vidyashilp University shall provide email services under the domain **@vidyashilp.edu.in** to its stakeholders either through its own infrastructure or through authorized third-party email service providers, based on operational requirements, security considerations, and resource availability.

In respect of staff members on exchange mode from one unit to another of Vidyashilp Domain, either for a short term or on long term assigned with **email id @vidyashilp.com** from the sister organisation and later absorbed at VU, etc., such staff members shall also abide by the policies as long as they serve in the VU.

Official email accounts (username@vidyashilp.edu.in) may be issued to University employees, students, research scholars, visiting/adjunct faculty, and any other individuals approved by the University Administration from time to time, strictly for official purposes.

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE

The following guidelines shall govern the use of university email services:

- University email accounts are the official mode of communication for academic, administrative, and institutional correspondence. Users are expected to regularly access and review their University email accounts.
- Official University communications, approvals, notifications, and institutional correspondence shall be conducted through authorized University email accounts.
- The email system shall not be used to create, transmit, store, or distribute disruptive, offensive, defamatory, discriminatory, threatening, or inappropriate content, including derogatory remarks relating to race, gender, disability, age, sexual orientation, religion, political beliefs, or national origin, as well as pornographic or unlawful material.
- Any user receiving such content from the University email account must immediately report the matter to the concerned supervisor, Reporting Manager, Head of Department, or competent authority.
- Users shall not impersonate another individual, forge email headers, or misuse another person's account credentials.
- Limited personal use of University email resources is permitted, provided such use does not interfere with official work, violate University policies, or consume excessive system resources. Personal emails should be stored separately from official correspondence.
- The circulation of chain mails, spam, unsolicited bulk messages, advertisements, or joke emails through University email accounts is strictly prohibited.
- Dissemination of virus alerts, malware warnings, official notices, or mass email communications by University users shall require prior approval from the competent authority.
- Auto-forwarding of University email to personal email accounts or external email services shall be prohibited unless specifically approved by the IT Department or competent authority.
- Users shall exercise caution while opening attachments, clicking external links, or downloading files from unknown or suspicious sources to prevent phishing attacks, malware infections, and unauthorized access.
- Users are responsible for maintaining the confidentiality and security of their account credentials and passwords. Sharing passwords or permitting unauthorized access to University email accounts is prohibited.
- Users are encouraged to use strong passwords and enable additional security measures such as multi-factor authentication (MFA), wherever supported.

VIDYASHILP UNIVERSITY ★ BANGALORE ★ REGISTRAR

- University email accounts shall not be used for unauthorized commercial activities, personal business promotions, political campaigning, or activities that may adversely affect the reputation of the University.
- Confidential, Restricted, examination-related, student, employee, financial, legal, or research information shall not be transmitted to unauthorized recipients through email.
- Users shall verify recipient addresses and distribution lists before sending emails containing sensitive institutional information.
- Users shall not upload or transmit Confidential or Restricted University information to public Artificial Intelligence (AI) services through email integrations, plugins, or external tools without authorization.
- Users are advised not to use the University email system for confidential personal correspondence, as the University reserves the right to monitor, audit, archive, or access email communications and related logs, where deemed necessary for security, legal, administrative, or operational purposes, subject to applicable laws and regulations.
- Email accounts and associated data remain the property of Vidyashilp University. The University reserves the right to suspend, deactivate, or revoke access to email services in cases of policy violation, security concerns, misuse, or upon cessation of association with the University.
- Upon separation from the University, email accounts may be disabled, archived, retained, or deleted in accordance with University retention requirements and operational procedures.

8. Anti-Virus

Vidyashilp University will ensure the protection of its computing infrastructure, systems, and network resources against viruses, malware, ransomware, spyware, and other cyber threats through the implementation of appropriate antivirus and endpoint security measures.

The following guidelines govern the use and management of antivirus protection within the University:

- All desktop computers, laptops, workstations, servers, and other computing devices procured or connected to the University network must have licensed and approved Anti-Virus (AV) and endpoint protection software properly installed, configured, and regularly updated.
- Antivirus software must be configured for automatic updates and scheduled scans at regular intervals to ensure protection against the latest threats and vulnerabilities.
- The University IT Department will oversee and monitor the overall protection of University systems and networks against viruses, malware, and other cybersecurity threats.

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE

- The IT Department will recommend, procure, deploy, and maintain appropriate endpoint security solutions and Gateway Anti-Virus systems for the University network infrastructure.
- Gateway Anti-Virus, email filtering, web security, and network threat protection mechanisms will be implemented on the University network to minimize the risk of malware propagation and unauthorized access.
- The IT Department, duly following the purchase procedure, will ensure timely renewal of antivirus licenses, subscriptions, and support services to avoid lapses in protection.
- Systems identified as infected, compromised, or suspected to contain malicious software must be immediately isolated or disconnected from the University network until the threat is completely removed and the system is verified as secure.
- Users must not disable, uninstall, bypass, or tamper with antivirus software, firewall settings, or other security controls installed by the University.
- Users must exercise caution while opening email attachments, downloading files, installing software, or accessing external storage devices to prevent malware infections and security breaches.
- External storage devices, including USB drives, external hard disks, and removable media, shall be scanned for malware before accessing or transferring data to University systems.
- Installation or use of unauthorized, pirated, or unlicensed software on University systems/network is strictly prohibited.
- Any activity intended to create, introduce, distribute, or facilitate malicious software or harmful code within University systems or networks, including viruses, worms, Trojan horses, ransomware, spyware, phishing tools, email bombs, or similar threats, is strictly prohibited.
- Any cybersecurity incident, suspected malware infection, data breach, or unusual system behavior must be promptly reported to the IT Department for investigation and remediation.

9. Network Access & Monitoring

Vidyashilp University will design, implement, and maintain its network infrastructure to provide secure, reliable, scalable, and high-performance connectivity for academic, research, administrative, and institutional activities while ensuring appropriate control over network access and usage.

All users accessing the University network, whether through wired, wireless, remote, or virtual access mechanisms, must comply with this policy and all related IT security guidelines issued by the University.

VIDYASHILP UNIVERSITY * BANGALORE * REGISTRAR

- The University reserves the right to monitor, log, audit, and analyze network traffic, device connections, authentication records, and system activity to ensure security, compliance, and operational stability. Routine monitoring may include traffic analysis, vulnerability checks, bandwidth monitoring, and security assessments.
- Users must not attempt to intercept, disrupt, bypass, or manipulate network communications, security controls, or monitoring systems.
- Only authorized and compliant devices may connect to the University network.
    - University-owned devices may access both wired and wireless networks.
    - Personal devices (laptops, tablets, smartphones) may access only the wireless network, subject to compliance.
    - Wired connection of personal devices requires prior approval from the IT Department.
    - All devices must have updated OS, licensed software, antivirus protection, and must be free from malware or vulnerabilities.
    - Non-compliant devices may be disconnected or blocked without notice.
    - Personally owned devices accessing University resources shall comply with the University's BYOD Policy and applicable security requirements.
    - The University may implement Network Access Control (NAC) or equivalent technologies to verify device compliance before granting network access.
- Every networked device must have a clearly identifiable owner or administrator responsible for its usage and security. Unmanaged or unidentified devices may be removed from the network.
- The IT Department will centrally manage IP address allocation through DHCP services across all network segments. Unauthorized DHCP servers, routing devices, or network control systems are strictly prohibited.
- Installation or use of Wi-Fi routers, access points, repeaters, or similar wireless devices on campus requires prior approval.
    - Only official University Wi-Fi networks may be used.
    - Unsecured or rogue wireless networks are prohibited.
    - Wireless networks must use secure authentication such as WPA2-Enterprise or higher with centralized authentication.
    - Sharing Wi-Fi credentials or unauthorized access is not permitted.
- Unauthorized VPN servers, SSH gateways, proxy services, tunneling tools, or remote access systems connected to the University network are strictly prohibited.

- Remote access to University systems must only be through approved VPN/secure access services.
- Remote access may be granted to authorized users based on institutional need and approval.
- All remote access activity will be logged and monitored.

- Network usage may be monitored to ensure fair usage, security, and performance.
  - Activities such as excessive bandwidth use, malicious traffic, unauthorized peer-to-peer sharing, and cryptocurrency mining are prohibited.
  - Misuse may result in restrictions, penalties, or suspension of access.
- Internet access may be filtered, restricted, or logged as per institutional policy and legal requirements.
  - Logs may include user identity, IP address, timestamps, and accessed resources.
  - Certain ports, services, and protocols may be restricted unless approved for academic or research use.
- Wireless network access requires secure authentication, and traffic must use approved encryption standards. Authentication and session logs may be maintained for security and auditing.
- Static IP addresses may be assigned only for approved servers or research systems.
  - Such systems must implement proper firewalling, access control, and security safeguards.
  - External access must not compromise internal network security.
- Special or unrestricted network access may be granted for approved academic, research, or operational requirements, subject to strict controls and IT Department approval.
- Network segmentation may be implemented to separate administrative, academic, research, examination, server, guest, IoT, and other network environments to improve security and operational resilience.
- Third-party vendors, consultants, contractors, and service providers requiring network access shall be granted only the minimum access necessary to perform approved duties and may be subject to monitoring and security controls.
- Any suspected network intrusion, unauthorized access attempt, denial-of-service activity, malware propagation, or network security incident shall be immediately reported to the IT Department for investigation and response.

10. Server Access & Maintenance

Vidyashilp University maintains a structured Server Access and Maintenance Policy to ensure that all institutional servers are securely managed, properly configured, and operated in a controlled environment. The policy defines ownership responsibilities, configuration standards, access controls, monitoring requirements, and compliance procedures to ensure system integrity, security, and reliability across all departmental and institutional servers.

- All internal servers must be owned and managed by an authorized operational group within the respective department/centre/section responsible for system administration.
- Any deviation from standard configurations must follow an exception approval and documented review process.
- Every server must have clearly identified ownership, including primary and backup administrators, system location, hardware/OS details, and application/function information.
- Server configuration and management information must be accurate, updated, and maintained at all times.
- Server logs must be maintained securely for a minimum period of three months or as specified by institutional policy.
- Static external IP addresses may be assigned only for approved servers such as research systems, web services, or institutional applications, subject to IT approval.
- In exceptional cases, unrestricted internet access may be permitted for specific servers for research or operational needs, provided strict controls, firewalling, usage restrictions, and complete logging are enforced.
- Server configurations must follow approved OS and security guidelines, with unnecessary services and ports disabled wherever possible.
- Access to server services must be logged and protected using appropriate access control mechanisms.
- Security patches and updates must be applied regularly and without delay.
- Principle of least privilege must be strictly followed; administrative/root access must be used only when required.
- Servers must be installed only in secure, access-controlled environments and not in open or unsecured areas.
- All critical security events must be logged, retained, and monitored, with defined retention periods for online logs and backups (daily, weekly, and monthly archives).
- Security events such as unauthorized access attempts, port scans, or system anomalies must be reviewed and reported by the IT/Information Security team with corrective actions.

- Servers must be regularly updated, and unnecessary network ports must be blocked through firewall rules.
- Intrusion detection systems must be enabled to detect suspicious activity and unauthorized changes in network identity or configuration.
- Regular audits will be conducted by authorized University bodies to ensure compliance with this policy, and findings will be addressed promptly without disrupting operations.
- The University in collaboration with Industry, R&D institutions, Funding Agencies may establish R&D Centre(s) with GPU installed within the campus. All the concerned including faculty/students/researchers shall abide by the IT Policy, applicable governing laws while using such IT devices.

11. Compliances:

- All Users shall mandatorily comply with the applicable existing provisions or amendments issued under the Information Technology Act, 2000 (as amended), Digital Personal Data Protection (DPDP) Act, 2023, cybersecurity regulations, copyright laws, licensing agreements, State Government regulations, Central Government regulations, and other applicable legal, statutory, contractual, or regulatory requirements from time to time.
- All Users shall adhere to the Standard Operating Procedures (SOPs), Policies, Standards, Guidelines, Circulars, or Official Notifications issued by the Competent Authority of Vidyashilp University from time to time.
- Violation of any of these stated in the policy may result in suspension of network access, device disconnection, financial penalties, disciplinary action including termination of employment/admission, or legal proceedings as deemed appropriate by the University.
- Any violation involving unauthorized access, data breaches, examination-related information, intellectual property, research data, cybersecurity incidents, or misuse of University ICT resources may be investigated and acted upon in accordance with applicable laws, University regulations, disciplinary procedures, and contractual obligations.
- The University reserves the right to conduct audits, reviews, inspections, and compliance assessments of ICT resources, systems, records, and activities to verify adherence to this Policy and related institutional requirements.

Disclaimer

This policy is subject to periodic review, monitoring, and updates by the University. Amendments may be made from time to time to reflect changes in technology, regulatory requirements, security practices, or institutional needs. All such revisions will take effect upon official communication through designated University channels.

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE