

TEMPLE UNIVERSITY
POLICIES AND PROCEDURES

Title:	Technology and Software Usage
Policy Number:	04.71.11
Issuing Authority:	Office of the President
Responsible Officer:	Vice President for Information Technology
Date Created:	November 2002
Date Last Amended/Reviewed:	March 5, 2026
Date Scheduled for Review:	March 2030
Reviewing Offices:	Information Technology Services

I. Scope of Policy & Rationale

This policy applies to all technology resources connected to the university network; all users of those resources, including faculty, staff, students, contractors, vendors, and affiliates; and all university computing facilities, data centers, and processing environments. It covers the direct and indirect use of university technology resources both on campus and off-campus, including the use of licensed software.

This policy also applies to personally owned devices (e.g., laptops, tablets, mobile phones) that connect to the university network or access university data, as well as cloud services, SaaS applications, third-party hosted systems, and external platforms used to store, process, or transmit university data.

The purpose of this policy is to protect the confidentiality, integrity, and availability of the university's data, electronic information, and supporting technology infrastructure. It establishes the security requirements, responsibilities, and restrictions governing the appropriate access and use of university technology resources. All users, as defined in this policy, are required to comply.

The university may monitor the use of its technology systems and resources for operational, security, and compliance purposes. Users should have no expectation of privacy when using university-owned or university-managed systems.

Violations of this policy may result in (i) suspension or revocation of an individual's computer account or other technology privileges; (ii) disciplinary action under applicable policies for faculty, staff, administrators, or students; and/or (iii) civil or criminal penalties under federal or state law. The university reserves the right, in its sole discretion and without limitation, to limit, restrict, suspend, or terminate access to technology resources for any account holder for any reason.

II. Policy Statement

All users are responsible for any technology resources provided by the university and for complying with this policy, including but not limited to:

- a. Account Holders shall access only those resources authorized by the University as defined by the Information Technology Services' System Access by University Enterprise Role

https://its.temple.edu/sites/its/files/imce/Policy_P60_System_Access_Grid.pdf).

- b. Account Holders may not use technology resources in connection with activities prohibited by any applicable university policy or by any applicable laws, ordinances, rules, regulations, or orders of any public authority having jurisdiction.
- c. Account Holders are prohibited from disclosing their own password to anyone and may not search for, access, copy or use passwords of others.
- d. Account Holders may not use technology resources to misrepresent themselves as another individual.
- e. Account Holders may not attempt to gain access to technology resources which they are not specifically authorized to access or assist others to do the same.
- f. Accounts cannot be shared, transferred to, or used by other users. Account Holders may not access or copy the directories, programs, files, data, or documents of other Account Holders without the permission of the applicable Account Holder.
- g. Shared or generic accounts, intended to be used by more than one user, are not permitted without prior written authorization from the Chief Information Security Officer or their designee.
- h. Once an account becomes inactive due to retirement, resignation, termination of employment, expulsion, withdrawal, graduation, end of contract or otherwise; University data may be transferred to the supervisor of the Account Holder after obtaining permission from, and at the sole discretion of, the cognizant Vice President/Dean, the Chief Information Security Officer, and Vice President for Information Technology.
- i. Software may only be used in compliance with applicable license and purchasing agreements.
- j. Account Holders must have prior written permission from the Vice President for Information Technology to remove or copy any technology resource owned or licensed by the university.
- k. Account Holders may not use technology resources to send, forward, or otherwise disseminate nuisance messages, messages that would constitute a violation of the university's policies and messages to a recipient who has previously notified the individual that such messages from the sender are not welcome.
- l. Account Holders may not impede, interfere with, or otherwise cause harm to others or their activities or create or constitute an unacceptable burden on technology resources as determined by Information Technology Services.

- m. Account Holders may not use or permit another person or entity to use technology resources for non-university business.
- n. Account holders must not send confidential or sensitive data to external recipients via email without encryption. Email should not be considered a personal communication channel. The University reserves the right to monitor, access, and review email communications in accordance with applicable laws, policies, and investigative requirements. Information Technology Services recommends that account holders not use their @temple.edu email accounts for personal purposes.
- o. Account Holders may not run unauthorized network services or servers, including but not limited to email servers, DHCP servers, DNS servers, authentication services, or file-sharing services, without prior written authorization from the Chief Information Security Officer or their designee.
- p. Account Holders may not store, transmit, or process sensitive, confidential, or regulated university data—including but not limited to FERPA-protected data, HIPAA-regulated data, export-controlled data, financial information, or protected research data—on personal devices, unapproved cloud storage, or unencrypted systems.
- q. Account Holders may not attempt to disable, bypass, or otherwise circumvent security controls established by the university, including but not limited to antivirus, endpoint protection, encryption, MFA, logging, monitoring, or data-loss prevention technologies
- r. The use of a personally owned computer or other personally owned device in conjunction with university technology resources (e.g., the university network) shall be governed by this Technology and Software Usage policy.
- s. Account Holders are strictly prohibited from using packet-capturing (“sniffing”) software, anonymizers, keystroke loggers, or any other device or software product that can be used to circumvent security controls. Additionally, Account Holders may not engage in unauthorized network scanning, monitoring, interception, probing of network traffic or systems, or attempt to discover vulnerabilities on any university system without prior written authorization from the Chief Information Security Officer or their designee. Nothing contained in this policy shall create: (i) an Account Holder’s entitlement to software, (ii) an obligation for the university to acquire software, (iii) a delegation of authority to any individual to acquire software on behalf of the university; or (iv) liability on the part of the University for an Account Holder’s noncompliance with this policy.
- t. Account Holders are responsible for physically securing university-owned or university-managed devices and must take reasonable measures to prevent loss, theft, or unauthorized access, including locking screens and securing devices when unattended.
- u. Account Holders must promptly report any suspected security incident, account compromise, loss or theft of devices, unauthorized disclosure of university data, or suspicious activity to the Office of Information Security.
- v. The university and its agents (i) shall have the right to audit all university- provided resources

to ascertain compliance with this policy and (ii) may permit software licensors and their agents to audit some or all technology resources to ascertain compliance with their license or other applicable agreements.

III. Security

- a. Technology resources may not be used to circumvent any security measures of the university.
- b. All devices connected to the university network that are capable of supporting anti-virus software must have the latest Information Technology Services-approved anti-virus/endpoint protection software and be updated on a regular basis (generally within seven days).
- c. All critical security patches must be tested and applied to operating systems, applications, and other software within 30 days of release. It is the responsibility of the system owner to keep systems and applications patched and protected. If the Office of Information Security identifies any system or application that is not in compliance with these requirements, the University reserves the right to remove the system from the network or take other appropriate actions to isolate the system and/or application until compliance is achieved or mitigating controls are approved.
- d. Information Technology Services has the right to perform security assessments on any software or device that utilizes the university network, including personal devices.
- e. All servers, computer installations and hosted systems must follow the security baselines established by Information Technology Services.
- f. All software applications, whether hosted on the university network or by a third party, that are intended to store, process, or otherwise handle confidential and/or sensitive data according to our data classification guidelines must be approved by the Chief Information Security Officer or their designee prior to the purchase.
- g. Information security tools/devices connected to the university network must be approved by the Chief Information Security Officer.
- h. All IP-capable devices installed on the university network shall have an IP address issued by Information Technology Services.
- i. All personnel responsible for publicly accessible computers must:
 - follow the shared computer software lockdown procedures (<https://its.temple.edu/policy-protection-publicly-accessible-computers>),
 - participate in the centrally managed Information Technology Services patching process,
 - attach keyboards using a locking mechanism,
 - enable encryption on wireless keyboards,
 - install proper secure screws on podium/instructor station security panels, and
 - use AccessNet username and password for authorization. The use of generic and/or local administrator accounts is prohibited except where access is only

provided to a desktop through automatic login on startup and where additional access to any network resources is limited through login/proxy access.

- j. Information Technology Services may filter network traffic to exclude peer- to-peer and anonymized traffic, malware, and unsolicited commercial e-mail, and otherwise to best ensure the efficient and effective operation of the university network.
- k. Access to all university data centers and telecommunication rooms shall be restricted to Account Holders properly authorized by Information Technology Services. All guests must sign in and out of all university data centers.
- l. Any incident of suspected hacking or intrusion attempts, compromised system, suspicion of password compromise, on-line harassment, or known violation of computer policy will be addressed pursuant to the instructions of the incident response team maintained by the Vice President for Information Technology (ciso@temple.edu).

IV. Privacy

- a. Account Holders must take all appropriate precautions to protect sensitive and confidential information stored on their systems.
- b. Computer systems and network devices may be monitored to ensure the security and protection of technology resources. In support of the goal of protecting privacy, all authority to log, intercept, inspect, copy, remove or otherwise alter any data, file, or system resource on Temple University's systems and traffic on Temple University's network rests with the Chief Information Security Officer and Vice President for Information Technology. The Chief Information Security Officer and Vice President for Information Technology may take action when, at his/her discretion, he/she determines that there is a potential or actual threat to the security or integrity of university computers, computer systems or networks or their authorized use. All such actions are subject to review by university counsel.
- c. All media (regardless of where the media resides) and systems that contain sensitive or protected data that is under the stewardship of the university must be protected in accordance with the Data Usage, Governance, and Integrity Policy (Policy [04.71.10](#)).
- d. All media taken out of service which contained protected or sensitive data, including remnant data, and any computer equipment taken out of service, must be purged of all data, or destroyed, by the university's Computer Recycling Center or an approved method authorized by the chief information security officer.

V. Software Licensing and Copyright

- a. **Licensed Software:** All university software must be used in accordance with its license agreement. Unauthorized copying or installation beyond the license terms is prohibited.
- b. **Pirated Software:** Use, installation, or possession of pirated or unauthorized software is strictly prohibited.
- c. **Copyright Compliance:** Users must comply with all applicable copyright laws and may not copy, distribute, or use copyrighted materials without permission.

VI. Definitions

- a. **Account Holders**
University faculty, staff, administration, students, non-Temple businesses who have a contractual relationship with the university, authorized individuals as outlined in Information Technology Services Guest Access policy, and other authorized individuals as approved by Chief Information Security Officer and Vice President of Information Technology. An individual who has been assigned credentials to access one or more technology resources.
- b. **Computers**
Includes, without limitation, mainframes, servers, mini-, micro-, super-, desktop, portable, laptop, and mobile computing devices such as smart phones, and all other electronic devices that connect to the university's networks.
- c. **Devices**
Includes, without limitation, mainframes, servers, mini-, micro-, super-, desktop, portable, laptop, and mobile computing devices such as smart phones and tablets, and all other electronic devices which connect to the university's networks.
- d. **IP Address**
A group of numbers that is used to uniquely identify a computer or other hardware connected to the university network.
- e. **Privileged Access**
An authorized user who has been granted rights or powers, typically reserved for the system administrator, on a computer system.
- f. **Shared or Generic Account**
An account that is used by more than one individual to access a technology resource.
- g. **System Administrator**
An individual who has been assigned the responsibility of administering and managing a computer application or server that performs functions beyond normal desktop or personal computing tasks. Systems administered by a system administrator usually support multiple users and administrators typically have privileged access.
- h. **Technology Resources**
Any one or more of the following in which the university has an ownership, lease, license, proprietary, managerial, administrative, maintenance or other legal or equitable interest: computers, devices, electronic communications systems, university network, data storage media, systems, terminals, printers, software, files, documentation, accounts, and any other hardware, software, information, or other technology attached or connected to, installed in, or otherwise used in connection or associated with any of the foregoing. The use of a device or other equipment that is not technology resources (e.g., a personally owned computer) in conjunction with technology resources (e.g., the university network) shall constitute the use of technology resources and shall be governed by this Technology and Software Usage policy (policy [04.71.11](#))

- i. University Network
All components that may be used to effect operation of university computer networks, including, without limitation, routers, switches, firewalls, computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures and other facilities, network electronics, telephone lines, modems, and other peripherals and equipment, data storage media, devices and systems, and software.
- j. Temple-Related Individuals
Temple students, employees, faculty, and applicants for employment and, certain other individuals associated with the university including, but not limited to, alumni, applications, trustees, volunteers, clients, temporary employees of agencies who are assigned to work for Temple University and third-party contractors engaged by Temple University and their agents and employees.
- k. Users
University faculty, staff, administration, students, non-Temple businesses that have a contractual relationship with the university, authorized individuals as outlined in Information Technology Services Guest Access policy, and other authorized individuals as approved by Information Technology Services.

Notes

1. History:

This policy supersedes and replaces the following policies, which are hereby rescinded:

Computer Usage Policy (04.71.11) adopted by the Vice President for Computer & Information Services on November 11, 2002, and updated on March 31, 2003, and February 23, 2006, and June 22, 2010.

Technology Usage Policy (which superseded the Computer Usage Policy, 04.71.11, and the Computer and Network Security Policy, 04.72.12) adopted by the Vice President for Computer & Financial Services and CIO on June 16, 2010.

Software Policy (04.71.12) adopted by the Vice President for Computer & Financial Services and CIO on June 16, 2010.

Policy for the Protection of Publicly Accessible Computers adopted by the Chief Information Security Officer on October 13, 2011.

Guidelines for the Secure Data Destruction of University Electronic Media Containing Confidential Information adopted by the Chief Information Security Officer on November 23, 2011.

Revised and modernized to reflect current university technology environments, including cloud services, SaaS applications, third-party hosted systems, personally owned devices, and contemporary cybersecurity practices. Updated provisions address account and access management, data protection, security controls, incident reporting, device security, software licensing, privacy, and technology resource monitoring on March 5, 2026.

Last Amended:

“Technology Usage Policy” adopted November 2002 and amended June 2010 Also, “Software Policy” adopted November 2002 and amended June 2010.

November 2022: Updated to reflect current Bylaws and job titles.

2. Cross References:

Student Conduct Code (Policy [03.70.12](#))

Policy Regarding Confidentiality of Student Records (Policy [03.20.11](#))

Granting Systems Access and Guest Cards to Guests
(<https://its.temple.edu/granting-systems-access-and-guest-cards-guests>).

Information Technology Services' System Access by University Enterprise Role
(https://its.temple.edu/sites/its/files/imce/Policy_P60_System_Access_Grid.pdf).

Data Usage, Governance, and Integrity policy (Policy [04.71.10](#))