TEMPLE UNIVERSITY
POLICIES AND PROCEDURES MANUAL

Title: Technology Usage
Policy Number: 04.71.11
Issuing Authority: Office of the Vice President for Computer & Financial Services and CIO
Responsible Officer: Vice President for Computer & Financial Services and CIO

Date Created: November 2002
Date Last Amended/Reviewed: June 16, 2010
Date Scheduled for Review: June 2014
Reviewing Office: Office of the Vice President for Computer & Financial Services and CIO

Scope of Policy & Rationale

This Temple University Technology Usage policy regulates the direct and indirect use of Technology Resources (defined below), both on-campus and off-campus.

The Computer Services Department provides the university community with computer systems and the network infrastructure to support instruction, research and administration. Access to technology resources is a privilege offered to University Users (defined below). Temple University reserves the right to revoke this privilege and/or take other disciplinary action against any individual who fails to comply with this Technology Usage policy.

Individuals are expected to be familiar with this Technology Usage before utilizing Technology Resources. Any of the following actions signifies that an individual has read this Technology Usage policy and agrees to comply with it: (i) signing an account application or the policy acceptance form, (ii) completing the computer account approval and acceptance process, (iii) any use of Technology Resources, or (iv) checking "I Agree" when changing a password on the TUsecure website. Violations of this Technology Usage policy may result in: (i) suspension or revocation of an individual's computer account and other computer privileges, (ii) disciplinary action as described in the Student Code of Conduct (copies available from the Student Center or Student Affairs Office), (iii) disciplinary procedures under the relevant policies for faculty, staff, administration, and students, and/or (iv) civil or criminal prosecution under federal and/or state law. Penalties under such laws may include fines, orders of restitution, and imprisonment.

Purpose/Scope of Policy

This policy sets forth guidelines to protect the confidentiality, availability and integrity of Temple University's data, electronic information and supporting infrastructure.

This policy establishes appropriate security requirements and restrictions on accessing and using the university's technology resources.

This policy covers all Technology Resources, all technology resources connected to the Temple network, all users of such systems, and to all university computing facilities, data centers and processing centers.

Definitions

a. Access Control List – a technology control that restricts, by user, the electronic information assets and technology resources that a user is allowed to access.

b. Account Owner – an individual who has been assigned credentials to access one or more technology resources.

c. Authorized Access - access by an authorized individual to technology resources in a manner that is appropriate for the given circumstances.

d. Computers – includes, without limitation, mainframes, servers, mini-, micro-, super-, desktop, portable, laptop, and mobile computing devices ("MCDs") such as smart phones; and all other electronic devices which connect to the university's networks.

e. Data Steward – a defined business unit leader who is responsible for the protection and safeguarding of the university's information assets and has been designated as the gatekeeper for specified data stored on technology resources. The data steward is responsible for assuring data quality, managing appropriate access, and working with the Data Standards and Oversight Committee to define data standards.

f. Electronic Communications Systems – Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications or technology resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes. Further, an electronic communications system means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such

communications. Examples include, but are not limited to, the Internet, intranet, electronic mail services, GPS systems, cell phones and MCDs.

g. Electronic Information Asset – an electronically stored information resource that, as a portion or whole, makes up a field, record, file, document, image, database, report, or other useful information.

h. IP Address - a group of numbers that is used to uniquely identify a computer or other hardware connected to the university network.

i. Local Security Protections - security options that can be set on an individual technology resource.

j. Non-public Technology Resources – A Technology Resource that is restricted to users who have been granted authorized access and that is not available for general usage. These Technology Resources are typically managed with access control lists.

k. Protected Information – Electronic information assets that have specific legal protection and are covered by the Pennsylvania Breach of Personal Information Act or other related laws. Protected data includes: social security numbers, financial account numbers, drivers' license numbers, and debit and credit cards with associated pin and/or security codes, or other data protected by law.

l. Shared or Generic Account - an account that is used by more than one individual to access a technology resource.

m. System Administrator – an individual who has been assigned the responsibility of administering and managing a computer system or server that performs functions beyond normal desktop or personal computing tasks. Systems administered by a system administrator usually support multiple users.

n. 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, electronic communications systems, university network, data storage media, devices and 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 computer 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 Usage policy.

o. 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

p. University Users –University faculty, staff, administration, students, and other authorized individuals as outlined in Computer Services Guest Access policy.

q. Workforce Member – an employee, guest, vendor or contract worker who has been granted access to technology resources.

I. Accessing Technology Resources

a. Individuals may apply to use Technology Resources so long as they qualify as a university user and comply with this Technology Usage policy. Users who are not university users are not permitted access to non-public Technology Resources. Questions regarding authorization and permitted uses must be referred to the chief information security officer at ciso@temple.edu.

b. Guest access to Technology Resources may be temporarily granted in accordance with Computer Services' Guest Access policy.

c. Individuals may not attempt to gain access to Technology Resources which they are not specifically authorized to access. Attempting to gain unauthorized access or assisting others in gaining unauthorized access to such Technology Resources is strictly prohibited and may result in disciplinary action up to and including termination of employment or dismissal from the university.

d. Individuals are prohibited from disclosing their own password to anyone. Individuals must safeguard their account and its contents and will be responsible for any misuse. Individuals may not search for, access, copy, or use passwords of others. Individuals may not use Technology Resources to misrepresent themselves as another individual. If an individual is a victim of such misrepresentation, upon discovery she or he must immediately report the incident to the chief information security officer in the Computer Services Department.

e. Individual accounts cannot be shared, transferred to or used by other users. Individuals may not access or copy directories, programs, files, data, or documents that do not belong to them without the permission of the account owner.

f. 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.

g. The account owner is responsible for all actions performed on Technology Resources through the account owner's account. The university reserves the right to hold an account owner liable if, through negligence or deliberate action, Technology Resources are misused in any way by the account owner or anyone using the account owner's account.

h. Once an account becomes inactive due to retirement, resignation or termination of employment, all associated electronic data belongs to the university, including university-related files, all email, and all personal files not removed prior to the employee's last day of employment or provision of services. University data may be transferred to the supervisor of the employee after obtaining permission from, and at the sole discretion of, the vice president for computer services or university counsel. It will be the employee's responsibility to remove all personal (non-business) information prior to leaving. The university will make reasonable efforts to respect the privacy of exiting employees and, if practicable, only access business-related files and email. When an email account is retained by a former employee in accordance with this policy, the account owner must transfer all business-related emails to the supervisor and ensure that any new business-related email is promptly forwarded to the appropriate university recipient.

i. University users maintain access rights to Technology Resources in accordance with the Computer Services Access and Revocation guidelines, which are maintained by Computer Services.

j. Without limiting its rights in any way, the university specifically reserves the right, in its sole discretion, to limit, restrict, suspend or terminate any user's account or use of Technology Resources, for any reason.

II. Usage

a. Individuals must have prior written permission from the Computer Services Department to remove or copy any Technology Resource owned or licensed by the university. Individuals may not copy any software unless they are licensed by the software licensor to do so, or unless the software is from the Computer Services Department's public domain library. Individuals may not remove fixed Technology Resources from their designated places without first obtaining written permission of the Computer Services Department.

b. Individuals may not use Technology Resources to send, forward, or otherwise disseminate nuisance messages. Nuisance messages include, without

limitation, knowing or reckless distribution of unwanted messages, messages that would constitute a violation of the university's harassment policies and messages to a recipient who has previously notified the individual that any messages (or messages of a particular type) from the sender are not welcome.

c. Individuals may not use Technology Resources to impede, interfere with or otherwise cause harm to others or their activities or create or constitute an unacceptable burden on Technology Resources. Nonexclusive examples of such prohibited use include: activity that creates excessive network traffic or computing load (absent a compelling legitimate university research or instructional purpose), installing equipment that may interfere with the university network, misusing mailing lists, distributing "chain letters;" mail bombing (flooding an individual, group or system with unacceptably numerous or large e-mail messages), sending spam or commercial advertisements, intentionally spreading hoaxes regarding a computer virus, worm or similar threat, creating telnet or file transfer sessions of excessive number or duration, registering custom (non-Temple) domain names, maintaining unregistered or otherwise unauthorized servers, engaging in distributed processing (unrelated to Temple University education or research without prior written permission from the Computer Services Department), and creating unacceptably large files.

d. Individuals may not use or permit another person or entity to use Technology Resources (including without limitation processing power, memory, and connectivity to the Internet) for running online advertising, storing data or engaging in distributed processing, other than such uses which are in furtherance of a legitimate university research or instructional purpose.

e. Individuals may not use Technology Resources in connection with activities prohibited by any applicable Temple University policy or by any applicable laws, ordinances, rules, regulations, or orders of any public authority having jurisdiction including, without limitation, those concerning: patent, trademark, copyright (including, but not limited to, copyrights covering text, images, audio, and video), and other intellectual property, unauthorized use of a person's image, civil rights, commerce, computer usage, conspiracy, telecommunications, defamation, forgery, child pornography and privacy.

f. Temple University prohibits the use of peer-to-peer file sharing software and protocols. Use of this type of software will result in the disabling of the applicable network port and may lead to disciplinary action.

g. E-mail and other computer files (collectively, "files") should not be considered private, particularly in light of (i) the open nature of the internet and related technology and (ii) the ease with which files may be accessed, copied and distributed. Individuals must not send messages by e-mail or store information in computer files that are of a confidential or extremely personal

nature, including, without limitation, information protected by privacy laws such as FERPA or HIPAA. Individuals are prohibited from sending protected information by email other than through a business process approved in advance by the Office of the Chief Information Security Officer.

h. Use of any packet-capturing ("sniffing") software, keystroke loggers, or any other device or software product that, in the sole discretion of the Computer Services Department, can be used (or is deemed to be used) to circumvent security controls is strictly prohibited without written approval of the chief information security officer.

i. Individuals must comply with Administrative Policy #04.71.12, Temple University Software policy, and all other applicable policies related to Technology Resources.

III. **Security Controls**

a. All devices connected to the university network that are capable of supporting anti-virus software must have the latest Computer Services-approved anti-virus software and definition files and be updated on a regular basis (generally within seven days).

b. 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 patched and protected.

c. Computer Services has the right to perform security assessments on any software or device that utilizes the university network. Critical systems and applications will undergo annual testing.

d. Any system that has been compromised by a security breach shall undergo the incident response process defined by Computer Services. Individuals must contact the chief information security officer if they suspect their system has been breached.

e. All Technology Resources will be compliant with all laws, including, without limitation, laws relating to computer security.

f. All production systems maintained by Computer Services will undergo change management procedures before any changes to software, hardware or the operating system are performed.

g. All server and computer installations must follow the minimum security baselines established by Computer Service's department of Information Security. Servers intended to hold private and confidential information may

require additional approvals, and will require additional protections as determined by the chief information security officer.

h. Computer Services is responsible for configuring and managing the university network as well as all wired and wireless connectivity to the university network. Devices connected to the university network must be approved by Computer Services to ensure that the security and availability of our network is maintained.

i. The chief information security officer is responsible for determining the level of authentication required for remotely accessing systems containing sensitive or protected data.

j. All IP-capable devices installed on the university network shall have an IP address issued by Computer Services. Operating equipment that supports the issuance of IP addresses, such as Dynamic Host Configuration Protocol (DHCP), is prohibited without prior written approval from Computer Services.

k. Computer Services may filter network traffic to exclude malicious traffic on both an incoming and an outgoing basis. Malicious traffic may include malware and unsolicited commercial e-mail.

l. The purchase and use of information security tools including, but not limited to, firewalls, intrusion detection/prevention systems and security diagnostic/hacking tools must be pre-approved in writing by the chief information security officer.

m. Access to all university data centers and processing facilities shall be restricted to properly authorized users. Access is granted by the chief information security officer.

IV. **Privacy**

a. The privacy and security of files, electronic communications, and other information belonging to individual university users will be protected to the extent reasonably possible. However, computers, computer systems and networks generally and the university network specifically must never be considered private, particularly in light of (i) the open nature of the Internet and related technologies, and (ii) the ease with which files and data can be accessed, copied and distributed. Users 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. Log file data shall be protected to ensure the privacy of our users. In support of the goal to protect

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 vice president for computer and financial services & chief information officer. The vice president may take action when, at his sole discretion he 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 will be reviewed by university counsel.

c. All systems that contain sensitive or protected data that is under the stewardship of the university, including but not limited to, social security numbers, academic records, protected health information, and financial data, must be protected regardless of the media on which it resides. Use and storage of protected information must follow approved business processes that contain adequate technical controls to mitigate the risk of unauthorized disclosure. The university privacy officer will work with the chief information security officer to ensure that adequate protection mechanisms are in place.

d. All computer equipment taken out of service shall be purged of all data stored on the system and shall go through the process defined by the University Computer Recycling Center.

e. All media returning from back-up storage, to be passed to a different user or taken out of usage altogether shall be purged of all information contained therein. Media containing sensitive or protected information must be purged by the University Computer Recycling Center or an approved method authorized by the chief information security officer.

f. All software applications, whether hosted on university network or by a third party, that are intended to hold, process or otherwise handle protected information (including, but not limited to social security numbers) must be first reviewed by the chief information security officer and the university privacy officer prior to the purchase or implementation of application occurs. Such software applications must conform to federal, state or other regulatory requirements AS WELL AS university policy.

V. Responsibilities

All users of Technology Resources are responsible for performing their job activities aware of information security and privacy processes, policies, and controls put in place to protect Temple University's information assets. Computer policies and guidelines can be viewed at http://www.temple.edu/cs/policies/index.htm.

Notes

1. **Dates of official enactment and amendments:**
   November 2002. Amended June 2010 and renamed "Computer Usage Policy" to "Technology Usage Policy"

2. **History:**

   Supersedes:
   This policy supersedes the 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.

   This policy supersedes the Computer and Network Security Policy (04.72.12) adopted by the Vice President for Computer & Information Services on November 4, 2003, and consolidated with this policy on June 22, 2010.

3. **Cross References:**
   Temple University Software policy # 04.71.12
   Temple University Student Code of Conduct policy #03.70.12
   Computer Services' Guest Access policy
   Computer Services' Information Asset Steward policy