TEMPLE UNIVERSITY

POLICIES AND PROCEDURES MANUAL

Title: Computer and Network Security Policy
Policy Number: 04.72.12
Effective Date: November 4, 2003
Issuing Authority: Office of the Vice President for Computer & Information Services

Purpose/Scope of Policy

A. Purpose

The purpose of this policy is to establish appropriate security requirements and restrictions on accessing and using University computers, computer systems and networks and safeguarding University information.

B. Scope

This policy covers all University owned and maintained computers, computer systems, computer networks and electronic communications facilities, the users of all such systems and networks, all computers connected to the Temple network, and to all University computing facilities, data centers and processing centers.

This policy represents the minimum security requirements that must be followed and establishes the Vice President for Computer and Information Services as the Temple University officer responsible for the establishment of and carrying out computer and network security policy.

Definitions

a. Authorized access: An access by an authorized individual to a computer resource in a manner that is appropriate and work related.

b. Authorized modification: A change to any data or system, in any form, that is done for reasons that are both appropriate and work related, and that has been authorized by the appropriate University official.

c. Denial of Service (DOS): An intentional, organized effort that is designed to prevent, delay, or hinder the authorized access to computer or network resources.

d. Privileged access: An Authorized user who has been granted additional rights or powers, typically reserved for the system Administrator, on a computer system.

e. Generic account: An account that is used by more then one individual to access a system for the purpose of sharing data, files, or programs.

f. Local security protections: Security options that can be set on an individual system.

g. IP address: A group of four numbers, of a format similar to "127.256.384.1" that is used to uniquely identify a computer or other hardware connected to the university network.

h. Change control process: An orderly method of applying and tracking authorized modifications to software programs and operating systems that are designed to improve security or performance of the system, such as performing software updates and installing patches.

i. Account: A formal relationship between University Computer Services and a user of those services that allow the user to access and use university computer systems for legitimate academic or other university work. Accounts are established in accord with the provisions of university policies that govern access and use of these computer systems.

Policy

I. General

1. Appropriate security shall include protection against unauthorized access to, use of, copying or distribution of information; unauthorized modification or destruction of information; denial of service; and protection against unauthorized access of computers, computer systems and networks.

2. University computers and computer systems may be used and networks may be accessed only by individuals authorized by the University. Issuance of an account and access to any University system must be approved by an authorized University official. Questions regarding authorization and permitted uses must be referred to the Chief Information Security Officer.

3. Any attempt by an individual to gain privileged access, as defined in Definitions (d.), or access to any account or system not belonging to that specific individual, on any University system, is prohibited, unless approved by the Vice President for Computer and Information Services under Section III.3.b.

4. Individual accounts may not be transferred to or used by an individual other than the authorized individual account holder. Sharing accounts or passwords is prohibited.

5. Generic accounts, intended to be used by more then one user, shall not be allowed on any computer, computer system or network without prior written authorization from the Chief Information Security Officer.

6. Access to all University data centers and processing facilities shall be restricted to properly authorized users.

7. All University computers, computer systems and networks will be compliant with all laws, including, without limitation, laws relating to computer security.

8. The University shall not be liable for, and the user assumes the risk of loss or destruction of data or interference with files resulting from the University's efforts to maintain privacy, integrity and security of the University's computers, computer systems and networks.

II. Responsibilities

1. The Vice President for Computer and Information Services has responsibility for establishing and overseeing the implementation and enforcement of this Policy.

2. Any University representative who accesses a system under the authority in this Policy must make a good faith effort to protect the integrity and privacy of data within the system.

3. The Chief Information Security Officer is responsible for developing, implementing, and enforcing this Policy under the direction of the Vice President for Computer and Information Services, and for coordinating questions and issues relating to this Policy with appropriate University departments including Campus Safety Services, University Counsel, Internal Audits, and other University offices as appropriate, as well as outside law enforcement and governmental agencies.

4. Users of University computers, computer systems and networks are responsible for:
    a. Understanding and complying with all security and computer usage policies governing University computers, computer systems and networks.
    b. Making a good faith effort to protect the integrity and privacy of data within the University's computers, computer systems and networks.
    c. Maintaining the proper use of his/her account and any activity conducted using such account, including choosing safe passwords, protecting those passwords, and ensuring that all local security protections are set correctly.
    d. Ensuring the local security of any system the user connects to the University network.
    e. Reporting any possible security lapses on any University computer, computer system or network to the system administrator or the Chief Information Security Officer.
    f. Respecting the physical hardware and network configuration of University networks. No system user shall modify, limit, or extend the University network or network configurations on which his/her system resides without the written authorization of the Office of Computer Services ("Computer Services").

    g. Refraining from the alternation, installation, modification, and/or deletion of any software stored or executed on any Computers without the express permission of the owner.
    h. Refraining from the use of any University computer resource for any unlawful purpose, including, without limitation, infringement of intellectual property (including copyrighted materials).

5. System administrators have the same responsibilities as users. However, because of their position, system administrators have additional responsibilities and privileges for specific systems or networks. System Administrators are responsible for:
    a. Preparing and maintaining security procedures compliant with this Policy and other applicable information security policies and procedures.
    b. Taking reasonable precautions to guard against corruption or compromise of University computers, computer systems, or networks.
    c. Taking appropriate measures to prevent unauthorized use of the system users' files.
    d. Assuring that all hardware and software license agreements are current and in force.
    e. Assuring that University computers, computer systems and networks have appropriate back-up procedures and that there is an adequate disaster recovery and business continuity plan in place and tested.
    f. Limiting access to privileged supervisory accounts to the administrator, except as may be approved by the Vice President for Computer and Information Services.
    g. Putting in place a change control process before performing any work or installing any new software, including patches, on any information system that is serving users. If the change is major, this process must be documented in writing.

III. <u>Specific Rules</u>

1. <u>University Network</u>
    a. Computer Services is responsible for configuring and managing the University network as well as all wired and wireless connectivity to the University network.
    b. All remote access to any University system is subject to monitoring by Computer Services.
    c. All access to restricted systems requires authentication (e.g., insertion of username and password).
    d. University printers, print servers, and storage arrays shall not be accessible from the Internet without the prior written approval of the Chief Information Security Officer.
    e. All IP-capable devices installed on the University network shall have an IP address issued by Computer Services.

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

g. All wireless communications on the University network and all authenticated access to the University network servers (e.g. mail, secure web, file transfers, etc.) must follow the Computer Services standard encryption protocol.

2. Security Protections

a. Security patches shall be applied within 30 days of vendor release unless otherwise approved by the Chief Information Security Officer.

b. All computer equipment assigned IP addresses by Computer Services shall be protected by the University approved antivirus protector updated on a regular basis (generally within seven days).

3. Privacy and Security

a. The privacy and security of files, electronic communications, and other information belonging to individual University users shall be protected to the extent reasonably possible. However, computers, computer systems and networks generally and the University network specifically should never be considered fully 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 should take all appropriate precautions to protect sensitive and confidential information stored on their systems.

b. In support of our goal to support 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 Information Services. The Vice President may take action when, at his sole discretion and after consultation with University Counsel, 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 requests for such actions must be made in writing to the Vice President for Computer and Information Services.

c. 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 the University network or other computer or computer system, for any reason.

d. All computer equipment taken out of service shall be purged of all data stored on the system.

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.

f. The purchase of antivirus software for installation on University Computers must be pre-approved by the Chief Information Security Officer. The purchase and use of information security tools, including firewalls, intrusion detection systems and hacking tools must be pre-approved in writing by the Chief Information Security Officer.

Notes

1. **Dates of official enactment and amendments:**

Adopted by the Vice President for Computer & Information Services on November 4, 2003.

2. **History:**

none

3. **Cross References**

none