**POLICY STATEMENT**

# Computing and Information Network Acceptable Use

## SU Policy Number: 601-001.2

ORIGINATING OFFICE
Computing Technologies Center

PURPOSE
The following policy contains the governing philosophy for regulating the use of Shippensburg University's computing/information network facilities and resources. Access to the University's computing/information network facilities and resources is a privilege granted solely to Shippensburg University faculty, staff, registered students, those with special accounts, and individuals using public access computers. All users of the computing/information network facilities must act responsibly and maintain the integrity of these resources. The University reserves the right to limit, restrict, or extend computing/information network privileges and access to its resources.

SCOPE
This policy applies to the use of all computing and network activity at Shippensburg University.

POLICY
The primary use of computing/information network facilities is for academic, administrative, and research activities. Other non-restricted use such as entertainment is secondary and may be restricted when it interferes with the primary use.

The University's computing/information network policies include, but are not limited to, the list below:

1. An individual shall use only the computer or network ID that was assigned to him/her, unless multiple access has been authorized for the ID.
2. Users may use only the password(s) provided to them and shall not try in any way to obtain a password for another user's computer or network ID.
3. Attempting to disguise the identity of the account or machine you are using is prohibited.
4. Use of the University's network resources to gain or attempt to gain unauthorized access to remote computers is prohibited.
5. Any deliberate act which may seriously impact the operation of computers, terminals, peripherals, or networks is prohibited. Such acts include, but are not limited to, the following: tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.

6. Attempting to modify in any way a program or digital media which the University supplies for any type of use at its sites is prohibited.
7. No person shall knowingly run or install on any of the University's computer systems, or give to another, a program which could result in the eventual damage to a file, computer system, or information network, and/or the reproduction of itself. This is directed towards, but not limited to, the classes or programs known as computer viruses, Trojan horses, and worms.
8. No person shall attempt to circumvent data protection schemes or uncover security loopholes.
9. All persons shall abide by the terms of all software licensing agreements and copyright laws. In particular, unauthorized copying of copyrighted software is prohibited, unless the University has a site license specifically allowing the copying of that software. Furthermore, the copying of site-licensed software for distribution to persons other than Shippensburg University faculty, staff, and students, or the copying of site-licenses software for use at locations not covered under the terms of the license agreement, is prohibited.
10. Deliberate acts which are wasteful of computing/information network resources or which unfairly monopolize resources to the exclusion of others are prohibited. These acts include, but are not limited to, sending mass mailings or chain letters, creating unnecessary multiple jobs or processes, obtaining unnecessary output, or printing or creating unnecessary network traffic. Printing unnecessary multiple copies of any document including resumes, theses, and dissertations is also prohibited.
11. The following type of information or software cannot be placed on any University-owned computer system:
    a. that which infringes upon the rights of another person.
    b. that which may injure someone else and/or lead to a lawsuit or criminal charges; examples of these are: pirated software, destructive software, pornographic materials, and libelous statements.
    c. that which consists of any advertisements for commercial enterprises.
12. No person shall harass, intimidate, threaten, or stalk another person by using email or other electronic means.
13. Use of the University's computer/information network resources to monitor another user's data communications, or to read, copy, change, or delete another user's files or software, without permission of the owner, is prohibited.
14. Use of the University's microcomputers, workstations, or information networks must be related to a Shippensburg University course, research project, work-related activity, departmental activity, or for inter-personal communications. Use of these resources for personal or financial gain is prohibited.
15. Any network traffic exiting the University is subject to the acceptable use policies of the network through which it flows (Prepnet, NSFNET, SSHENET, etc.), as well as to the policies listed here.
16. Existing University policies such as the Sexual Harassment Policy, Student Disciplinary Code, Academic Dishonesty Policy, Facilities Use Policy, etc., listed in University publications, will be enforced as they relate to a violation of the Computer Use Policy.

## RESPONSIBILITIES

The Computing Technologies Center (CTC) and the President should be notified about violations of laws and policies governing information use, intellectual property rights, or copyrights, as well as about potential loopholes in the security of the University's computer systems and networks. The user community is expected to cooperate with the CTC in its operation of computer systems and networks as well as in the investigation of misuse or abuse. Should the security of a computer system or information network be threatened, suspected user files may be examined under the direction of the University President or his/her designee.

While the university recognizes the role of privacy in an institution of higher learning, and will endeavor to honor that ideal, there should be no expectation of privacy of information stored on or sent through university-owned IT resources, except as required by law. For example, the university may be required to provide information stored in IT resources to someone other than the user as a result of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. §67.101 et seq.). In order to provide system reliability, copies of all files are maintained on backup storage devices so that even the deletion of files by a user will not guarantee their destruction. The need for system maintenance and reliability may require University personnel to have access to user's files.

Those who do not abide by the policies listed above are subject to suspension of computer/information network privileges, disciplinary actions that may result in suspension or dismissal, and possible referral to the appropriate judicial process.

Offenders may also be subject to criminal prosecution under federal or state law, and should expect the University to pursue such action. As an example, under Pennsylvania law, it is a felony punishable by a fine up to $15,000 and imprisonment up to seven years for any person to access, alter or damage any computer system, network, software, or database, or any part thereof, with the intent to interrupt the normal functioning of an organization [18Pa.C.S.3933(a)(1)]. Disclosing a password to a computer system, network, etc., knowingly and without authorization, is a misdemeanor punishable by a fine of up to $10,000 and imprisonment of up to five years, as is intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software [18Pa.C.S.3933(a)(2) and (3)].

## PROCEDURES

## RECISSION

## APPROVALS

President's Cabinet 4/29/2004, Revised
President's Cabinet 8/31/2009, Revised

## FILENAME:

601-001.0 Computing and Information Network Acceptable Use

## DATE:

8/31/2009

## DISTRIBUTION:

Public