POLICIES: COMPUTER AND NETWORK POLICY (ACCEPTABLE USE)

Binghamton University Computer and Network Policy (Acceptable Use)

I. Introduction

Access to information technology is essential to the state university mission of providing the students, faculty and staff of the State University of New York with educational and research services of the highest quality. The Acceptable Use of Information Technology Resources policy (AUP) of Binghamton University provides for access to information technology (IT) resources and communications networks within a culture of openness, trust, and integrity. In addition, Binghamton University is committed to protecting itself and its students, faculty, and staff from unethical, illegal, or damaging actions by individuals using these systems.

II. Purpose

The purpose of this policy is to outline the acceptable use of information technology resources. These rules exist to protect and preserve the privilege of use for students, faculty and staff and to ensure that members of the university community have access to reliable and robust IT resources that are safe from unauthorized or malicious use.

III. General Principles

1. Use of the computing and network resources of Binghamton University shall be consistent with the education, research and public service mission of the State University of New York and consistent with this policy.

2. Eligible individuals are provided access in order to support their studies, instruction, duties as employees, official business with the university, and other university sanctioned activities. Individuals shall not share with or transfer to others their university accounts, including but not

limited to user IDs, passwords, or other mechanisms that allow them to gain access to university information technology resources.

3. This policy applies to all Binghamton University's computing and network resources, and external computing and networking resources accessed via Binghamton University's computing and networking resources.

4. The University reserves the right to limit access to its networks when applicable system or university policies or codes, contractual obligations, or state or federal laws are violated.

5. The University reserves the right to remove or limit access to material posted on university-owned computers when applicable system or university policies or codes, contractual obligations, or state or federal laws are violated.

6. Non-University-owned computers that house material which violates the University's policies are subject to network disconnection without notice.

7. Although the University does not generally monitor or restrict the content of material transported across networks, it reserves the right to access and review all aspects of its computing systems and networks, including individual login sessions and account files, to investigate performance or system problems, investigate information security incidents, or upon reasonable cause to determine if a user is violating this policy or state or federal laws.

8. Colleges, departments, and other administrative units are free to supplement this policy with additional guidelines, provided such guidelines are consistent with university policy.

IV. Unacceptable Use

1.Unauthorized use of intellectual property: Intellectual property rights such as patents and copyright exist to help promote the progress of science and the arts. Users must refrain from activities that violate intellectual property rights such as but not limited to:

> **a.** Except as provided by the principle of Fair Use, copying, distributing, displaying or publishing copyrighted material.
>
> **b.** Failure to respect and abide by the terms and conditions of software use and redistribution agreements.

2. Excessive non-priority use of information technology resources: Priority for the use of information technology resources is given to those activities related to the university's missions of teaching, learning and research. These resources are limited and demand is high. Individuals should exercise restraint and may be asked to abstain from using resources for purposes that fall outside the mission. Such activities may include but are not limited to:

a. Activities which degrade the performance of a computer system or network, use a system or network for which the user is not authorized, or deprive authorized users of resources or access to computers or networks is prohibited.

b. Extensive and/or disruptive use of computing or network resources for recreational gaming or other entertainment purposes. Recreational game players occupying a seat in a public computing facility must give up the use of the device when others who need to use the facility for academic or research purposes are waiting.

c. Generating excessive network traffic, including spamming, certain file-sharing applications and denial-of-service, is prohibited.

3. Unacceptable system and network activities: Users are prohibited from engaging in any activity that violates system or university policies or codes, contractual obligations, or state or federal laws. Unacceptable activities include but are not limited to:

a. Using the information technology resources of Binghamton University for private commercial purposes or for financial gain.

b. Using the information technology resources of Binghamton University to engage in illegal activity.

c. Accessing, viewing, copying, altering, or destroying data for which authorization has not been granted.

d. Engaging in activities intended to obscure or hide a user's identity.

e. Sharing with, or transferring to others, a user's university accounts, user IDs, passwords, or other mechanisms that allow them to gain access to university information technology resources.

f. Running or otherwise configuring software or hardware to intentionally allow access by unauthorized users or acquire unauthorized data. Individuals must configure hardware or software in a way that reasonably prevents access by unauthorized users.

g. Using facilities, accounts, access codes, privileges or information for which they are not authorized in their current circumstances. When a user ceases to be a member of the university community or is assigned a new position and/or responsibilities within the State University system, the user's access and authorization must be reviewed.

h. Attempting to circumvent or subvert any system's security measures. Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

4. Misuse of electronic communications: Electronic communications are essential to carrying out the university mission and for communication among faculty, staff, students, and their correspondents. Users must refrain from activities that abuse these tools such as:

a. Using the university's information technology resources to libel, harass, or slander any other person.

b. Propagating chain letters or spam.

c. Masquerading as or impersonating someone else by using their email address

d. Monitoring the electronic communications of others.

5. Political Advertising or Campaigning: The use of Binghamton University's computers and networks shall be in accordance with University policy on use of University facilities for political purposes (Binghamton University's Campus Visits by Candidates for Political Office).

V. Rights and Responsibilities

1. The issuance of a password or other means of access is intended to assure appropriate confidentiality of the University's files and resources and does not guarantee privacy for use of university equipment or facilities.

2. The University provides reasonable security against intrusion and damage to files stored on the central facilities, and provides for some archiving of files based upon the operational needs of the University. However, the University is not responsible for the loss of users' files or data. Users should take their own steps to backup and protect important information.

3. Users should be aware that the University's computer systems and networks might be vulnerable to unauthorized access or tampering. In addition, computer files, including e-mail, may be considered "records" which may be accessible to the public under the provisions of the New York State Freedom of Information Law.

4. E-mail messages are not personal and private. The university as a practice does not monitor or restrict content of material transmitted on the university network or posted on university-owned computers, but reserves the right to limit or remove access to its networks and to material posted on its computers, when applicable university policies or codes, contractual obligations, or state or federal laws are violated. Program managers and technical staff may access a student or employee's e-mail:

- For a legitimate business purpose (e.g. the need to access information when an employee is absent),
- To diagnose and resolve technical problems involving the system, and/or

- To investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

5. E-mail messages sent/received in conjunction with University business may:

- Be considered state records under applicable state regulations;
- Be releasable to the public under the Freedom of Information Law;
- Require special measures to comply with the Personal Privacy Protection Law.

6. All E-mail messages including personal communications may be subject to discovery proceedings in legal actions.

VI. Sanctions

Violators of this policy may be subject to immediate suspension of services by Information Technology Services and to the existing student or employee disciplinary procedures of Binghamton University. Sanctions may include the loss of network access and computing privileges. Illegal acts involving Binghamton University's computing resources may also subject users to subpoena and prosecution by commercial enterprises, local, state and/or federal authorities.