Binghamton University Foundation
Acceptable Use of Information Technology Resources Policy

Last Updated 6/1/2018

I. Introduction

Access to Binghamton University Foundation (the Foundation) information technology and computing resources is essential to achieving the Foundation's mission. The Foundation is committed to protecting itself and its alumni, donors, staff, volunteers and friends from unethical, illegal, or damaging actions by individuals using these systems.

Users of these services and facilities have access to valuable Foundation resources, to sensitive data, and to internal and external networks. Consequently, it is important for users to behave in a responsible, ethical, and legal manner.

II. Purpose

The purpose of this policy is to outline the acceptable use of BU Foundation information technology resources. This policy exists to ensure that members of the Foundation's community have access to reliable and robust IT resources that are safe from unauthorized or malicious use.

III. Scope

This policy applies to all users of information technology and computing resources owned or managed by the Foundation. Individuals covered by the policy include (but are not limited to) Foundation and University staff, faculty, visiting faculty, students, alumni, volunteers, guests or agents of the administration, external individuals and organizations who have been granted access to Foundation data or technology.

Computing resources include all Foundation owned, licensed or managed hardware and software regardless of the ownership of the computer or device.

IV. General Principles

In general, acceptable use means respecting the rights of other computer users and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the user will face disciplinary action, including the restriction and possible loss of privileges. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

Access to Foundation files or information will be approved by authorized personnel when there is a valid reason to access that information. Authority to access Foundation technology resources will be granted by the Director of Foundation Information Technology in conjunction with senior management of the Foundation. External law enforcement agencies may request access to files through valid subpoenas and other legally binding requests. As a 501(c)(3) corporation, the Foundation is not a state agency and not subject to FOIL. All such requests will be reviewed and approved by the Foundation's legal Counsel.

Users are individually responsible for appropriate use of all resources assigned to them, including the computer, the network address or port, software and hardware. Authorized Foundation users may not enable unauthorized users to access Foundation resources.

1. Use of the computing and network resources of the Foundation shall be consistent with the mission of the Binghamton University Foundation and this policy.
2. Eligible individuals are provided access in order to support their duties as employees, official business with the Foundation, and other Foundation sanctioned activities. Individuals shall not share with or transfer to others their Foundation accounts, including but not limited to user IDs, passwords, or other mechanisms that allow them to gain access to Foundation information technology resources.
3. The Foundation reserves the right to limit or withdraw access to resources when applicable system or Foundation policies or codes, contractual obligations, or state or federal laws are violated.
4. The Foundation reserves the right to remove or limit access to material posted on Foundation owned or managed computers when applicable system or Foundation policies or codes, contractual obligations, or state or federal laws are violated.
5. Although the Foundation does not generally monitor or restrict the content of material stored on or accessed using Foundation resources, it reserves the right to access and review all aspects of its computing resources, including individual login sessions and account files, to investigate performance or system problems, investigate security incidents, or upon reasonable cause to determine if a user is violating this policy or state or federal laws.
6. Installation of software on Foundation computers shall be limited to a standard configuration and other software necessary for the performance of the employee's job. This shall be determined in consultation with the employee and her/his supervisor. Installation and support of all software will be the responsibility of the Foundation's IT staff.

V. Unacceptable Use

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

1. Using the information technology resources of the Foundation for personal or private commercial purposes or for financial gain.
2. Activities that would jeopardize the Foundation's tax-exempt status, including political activities
3. Using the information technology resources of the Foundation to engage in illegal activity.
4. Accessing, viewing, copying, altering, or destroying data for which authorization has not been granted.
5. Engaging in activities intended to obscure or hide a user's identity.
6. Sharing with, or transferring to others, a user's accounts, user IDs, passwords, or other mechanisms that allow them to gain access to the Foundation's information technology resources.
7. Running or otherwise configuring software or hardware to intentionally allow access by unauthorized users or acquire unauthorized data.
8. 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

Foundation's community or is assigned a new position and/or responsibilities within the Foundation, the user's access and authorization must be reviewed.

9. 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.
10. Using any automated processes to gain technical advantage over others is explicitly forbidden.
11. Installing or otherwise altering the software or hardware on Foundation owned or managed computers without the explicit permission of Foundation IT.

The Foundation may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

VI. Data Confidentiality

Data is a valuable resource of the Foundation, and some data must be protected with a higher level of attention and caution. The level of protection is based on the method defined by the **Data Classification Policy.**

VII. Passwords

Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data. Password use must therefore adhere to the policy statement found below.

1. To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must **never** be used as a user ID or a password.
2. All passwords are to be treated as sensitive information and should therefore never be written down or stored on-line unless adequately secured.
3. Passwords should not be inserted into email messages or other forms of electronic communication without the consent of the Director of Foundation Information Technology
4. The same password should not be used for access needs external to the Foundation (e.g., online banking, retail websites, personal email accounts, benefits, etc.).
5. Individual passwords should not be shared with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent of the Director of Foundation Information Technology or the senior management of the Foundation and must have a primary responsible contact person. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those passwords, and that person will ensure that only appropriately authorized employees have access to the passwords.
6. If a password is suspected to have been compromised, it should be changed immediately and the incident reported to the Director of Foundation Information Technology.

Additionally, passwords to Foundation resources must meet certain minimum standards. These standards may change as necessary and will be communicated and enforced by the individual resources they protect.

VIII. Email Communication

1. Security and Privacy of Email

Email messages are not personal and private; therefore, all email users should exercise extreme caution in using email to communicate confidential or sensitive matters.

a. **Confidential Information**
Email is not considered a secure mechanism and should not be used to send information that is not considered public. Confidential and Restricted Information, as defined in the Foundation's **Data Classification Policy**, should not be communicated via email unless absolutely necessary and approved by the Director of Foundation Information Technology. Credit card information and Social Security Numbers may NEVER be communicated via email.

b. **Compromised Accounts**
An email account which has been used for Foundation business and has been compromised, whether through password-cracking, social engineering or any other means, must be immediately reported to the Director of Foundation Information Technology and promptly remedied. Remediation will include a password reset, review of account settings, computer scans and malware disinfection to prevent possible leakage of personally identifiable information, spamming, potentially infecting others, etc.

IX. User Responsibilities

As a member of the Foundation community, the Foundation provides users with the use of work-related tools, including access to certain computer systems, technology, hardware, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet.

Users are responsible for knowing the regulations and policies of the Foundation that apply to appropriate use of these technologies and resources. Users are responsible for exercising good judgment in the use of the technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

As a representative of the Foundation, users are expected to respect both the Foundation and University's good names in electronic dealings.

X. Adherence with Federal, State, and Local Laws

As a member of the Foundation's community, users are expected to abide by applicable local ordinances and state and federal law. Some guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

This policy is not to be interpreted so as to interfere with federal, state or local laws. In such case where federal, state or local laws conflict with this policy, the law will supersede this policy.

As a user of the Foundation's computing and information resources users must:

1. Abide by all federal, state, and local laws.
2. Abide by all applicable copyright laws and licenses. The Foundation has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.
3. Observe the copyright law as it applies to music, videos, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.
4. Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

XI. Privacy and Personal Rights

1. All users of the Foundation's technology resources are expected to respect the privacy and personal rights of others.
2. Do not access or copy another user's email, data, programs, or other files without the written permission of the Director of Foundation Information Technology or senior management of the Foundation.
3. Although the Foundation does not generally monitor or restrict the content of user files, email or electronic communications, it reserves the right to access and review all aspects of its computing systems and networks, including individual login sessions, email and files, to investigate performance or system problems, investigate security incidents, or upon reasonable cause to determine if a user is violating Foundation policy or state or federal laws
4. While every effort is made to insure the privacy of Foundation email users, this may not always be possible. In addition, since employees are granted use of electronic information systems and network services to conduct Foundation business, there may be instances when the Foundation, based on approval from authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user.
5. Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to discipline as well as legal action by those who are the recipient of these actions.

XII. User Compliance

By accessing Foundation computing resources or accepting any Foundation issued computing accounts, users are agreeing to comply with this and all other computing related policies. Users have the responsibility to keep up-to-date on changes in the computing environment, as published, using electronic and print publication mechanisms, and to adapt to those changes as necessary.

Users will be required to review and sign the current applicable technology policies annually.

XIII. Binghamton University Foundation Resources

Data Classification Policy
Non-Disclosure agreement
Volunteer Agreement
Credit Card Handling Policy
Credit Card Terminal Use and Handling Policy
Binghamton University Mass Communication Policy

I have read and understand the terms of this agreement.

Print name: ____ Date: ____________________

Signature: ____

Department: ____

Supervisor Name:____