Acceptable Use of Information Technology Resources Policy

PURPOSE

The purpose of this policy is to define the acceptable use of Fitchburg State University's (FSU) applications, hardware, information and other information technology resources and systems.

SCOPE

This policy applies to any person utilizing FSU's information technology resources. The following persons are authorized to use FSU information technology resources: (1) current faculty; (2) current staff; (3) current students; and (4) authorized visitors.

POLICY

Acceptable use of FSU information technology resources includes usage for academic, educational or professional purposes which are directly related to official FSU business and in support of FSU's mission. Accordingly, users are encouraged to utilize FSU's information technology resources to the fullest extent in pursuit of the University's mission, goals, and objectives. The University expects that these information technology resources are always utilized in a responsible manner and reserves the right to limit or remove access as needed.

FSU's electronic communications systems, including Internet, telephony, email, and messaging services, are to be used primarily for university-related purposes. **Users shall have no expectation of privacy over any communication, transmission, or work performed using or stored on FSU's information technology resources.** The University reserves the right to monitor any and all aspects of its information technology resources and to do so at any time, without notice, and without the user's permission. FSU makes no warranties, expressed or implied, for the information technology resources it is providing. FSU will not be responsible for any damages a user may suffer, including loss of data, undelivered messages or content, or service interruptions. FSU denies any responsibility for the accuracy or quality of information obtained through its information technology resources.

Unacceptable use of the FSU electronic communications systems includes, but is not limited to, the following:

- Activities that violate local, state, or federal laws and/or regulations;
- Excessive, unreasonable, or unauthorized personal use;
- Storing, sending, or forwarding e-mails that contain libelous, defamatory, obscene, threatening, or harassing content;
- Infringing on intellectual property rights;
- For commercial purposes;
- Activities that attempt to circumvent or disable protection mechanisms that have been put in place by FSU;
- Utilize external media on the network which may contain viruses or malware.

For some specific examples of unacceptable uses of systems, see: ADDENDUM 1

Use of Technology

I. Access

Users of FSU's information technology resources are authorized to access only systems, including hardware and software, where access has been approved, per the ***Access Control Policy***.

II. Remote Access

Remote access is authorized for only those users with an approved business or academic use. Users who have been approved for remote access are responsible for adhering to the requirements defined in the FSU Remote Access Policy.

III. Media

Users shall not use media, such as flash drives or portable hard drives, until they have been scanned for viruses, spyware, malware, Trojans, or other similar threats to the security or functionality of FSU information technology resources.

IV. Data Encryption and Storage

Confidential and/or personally identifiable information (PII) must be protected by encryption. Encryption methods that have been approved and are listed in the FSU Encryption Policy should be utilized in these cases. Users who are unfamiliar with using approved encryption technologies should seek guidance from the FSU Helpdesk.

V. Cloud Computing and Storage

Advances in cloud computing offer convenient technology solutions such as data storage and connectivity. Data placed on any cloud computing storage solution must adhere to the same policies as data stored on FSU's internal technology resources.

Computer Virus and Malware Protection

It is important that users take particular care to avoid compromising the security of the FSU network. Users shall exercise reasonable precautions in order to prevent the introduction of a computer virus or other malware into the FSU network. Virus scanning software is installed on all FSU systems and is used to check any software downloaded from the Internet or obtained from any questionable source. Users are prohibited from disabling, or attempting to disable, virus scanning software. Users must scan portable media devices for viruses and malware before using them to ensure that they have not been infected. If users are unsure of how to utilize virus and malware scanning tools, they should contact the FSU Helpdesk for additional information.

Messaging Technologies

Use of email and other messaging technologies shall never be used to transmit confidential or sensitive information in an unencrypted format. Users must pay additional attention to email content and senders and must not open email attachments from unrecognized or suspicious senders. If there are questions about the security of an email, email attachment, or messaging technology users should contact the; FSU Helpdesk. For additional information on the use of email and messaging technologies at FSU, consult the Electronic Mail Services Policy.

Information Protection

Users may have access to confidential, sensitive, or public information. Refer to the FSU Information Classification Policy to understand what data falls into these three categories and how it should be protected. It is not permissible for users to acquire, or attempt to acquire, access to protected data unless such access as per the Access Control Policy. Under no circumstances may users disseminate any protected information, unless such dissemination is required.

Incident Response

The FSU IT staff is tasked with responding to all electronic information technology security related incidents, such as computer virus infections. In order to effectively respond to these events, the IT staff relies on timely information and reporting from users. Subsequently, users are required to contact the IT Security Officer or other FSU IT staff if:

- They observe unauthorized or suspicious activity;
- They know or suspect that a security incident has or is going to occur.

Password Use

Many of FSU's information technology resources require the use of a unique user account and password. It is important for FSU users to create strong passwords and protect these passwords. To this end, users must never share their passwords with anyone else, must maintain privacy of their password, and must promptly notify IT personnel if they suspect their passwords have been compromised. For additional information on password creation, use and protection, refer to the FSU Password Policy.

Physical and Environmental Security

Assistance from users is required to ensure a physically and environmentally secure working environment. Users are required to be aware of locking and access restriction mechanisms and must proactively challenge unidentified or unescorted personnel within restricted areas of the campus. Users who leave their devices unattended must log off or lock the system before leaving.

Problem Management

Users are required to report problems or issues discovered with FSU information technology resources to the FSU Helpdesk immediately following discovery.

Information Security Awareness Training

FSU employees may be required to attend security awareness training upon hire and at least annually thereafter. For additional information on FSU's Security Awareness program, refer to the Security Training and Awareness Policy.

ENFORCEMENT

Any person found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights, termination of employment or expulsion from the University.

ADDENDUM 1 – Some examples of Unacceptable Use

- Modifying system or network facilities, or attempting to crash systems or networks
- Using, duplicating or transmitting copyrighted material without first obtaining the owner's permission, in any way that may reasonably be expected to constitute an infringement, or that exceeds the scope of a license, or violates other contracts is prohibited and may subject the user to civil and criminal liabilities.
- The use of any peer to peer file sharing application is not permitted.
- Tampering with software protections or restrictions placed on computer applications or files.
- Using University technology resources for personal for-profit purposes.
- Sending messages that are malicious or that a reasonable person would find to be harassing.
- The operation of any type of SMTP server or service.
- Subverting restrictions associated with computer accounts.
- Using technology resources to obtain unauthorized access to records, data, and other forms of information owned, used, possessed by, or pertaining to the University or individuals.
- Accessing another person's computer account without permission. Users may not supply false or misleading data, or improperly obtain another's password to gain access to computers or network systems, data or information. Obtaining access to an account name or password through the negligence or naiveté of another is considered to be a specifically prohibited use.
- Intentionally introducing computer viruses, worms, Trojan Horses, or other rogue programs into information technology resources that belong to, are licensed to, or are leased by Fitchburg State or others.
- Physically damaging technology resources either purposefully or negligently.

- Using, or encouraging others to use, technology resources in any manner that would violate this or other University policies or any applicable state or federal law.
- Falsely reporting or accusing another of conduct that violates this policy, without a good faith basis for such an accusation.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Management Team	Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented. Review this policy periodically and update as needed in response to environmental and/or operational changes.
All Users	Understand and adhere to this policy. Use FSU resources in only those methods, which have been identified as acceptable by this policy. Immediately report unauthorized or suspicious activities or violations of this policy to their manager and the IT Information Security Officer.

REFERENCES

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201 - HIPAA	Supporting Standards and Procedures
DS5 Ensure System Security DS8 Manage Service Incidents		

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
1.0	1/12/2016	Compass ITC	Initial Draft

Version: 1.0

Issued: 1/12/2016