



USF Information Technology Security

Policies for all University Employees

Updated 11/2/2007

Contents

SECTION 1: OVERVIEW AND PURPOSE OF THIS POLICY	3
1.1 OVERVIEW.....	3
1.2 PURPOSE	3
1.3 DEFINITIONS.....	4
SECTION 2: GENERAL ACCEPTABLE USE POLICY	6
2.1 GENERAL POLICIES.....	6
2.2 AVAILABILITY	6
2.3. RIGHT TO MONITOR	6
2.4 SECURITY.....	6
2.5 LEGAL CONSIDERATIONS	7
2.6 ENFORCEMENT.....	7
SECTION 3: UNACCEPTABLE USE.....	7
3.1 UNACCEPTABLE AND PROHIBITED ACTIVITIES	7
SECTION 4: DATA MANAGEMENT.....	8
4.1 BACKUP POLICIES.....	8
4.2 STORAGE OF COPYRIGHTED MATERIAL ON USF MACHINES	9
4.3 INFORMATION HANDLING.....	9
SECTION 5: ACCESS POLICIES	11
5.1 USERNAME AND PASSWORD POLICIES.....	11
5.2 SUPERVISOR RESPONSIBILITIES.....	12
5.3 GUEST AND SPECIAL ACCESS	12
5.4 ACCESS AUDITS	12

SECTION 6: INTERNET AND INTRANET POLICIES	13
6.1 INTERNET SECURITY POLICY	13
6.2 INTRANET	13
6.3 WWW.SF.EDU WEBSITE POLICIES	13
SECTION 7: EMAIL POLICIES	13
7.1 EMAIL DEFINITIONS AND PURPOSE	14
7.2 CONTENT SCANNING.....	14
7.3 EMAIL VIRUS PROTECTION	14
7.5 SIZE LIMITS	14
7.6 EMAIL BACKUP	14
SECTION 8: SOFTWARE COMPLIANCE	14
8.1 SOFTWARE POLICY PURPOSE	14
8.2 SOFTWARE GUIDELINES.....	15
8.3 QUARTERLY AUDITS	16
8.4 PENALTIES AND REPRIMANDS	16
SECTION 9: TELECOMMUNICATIONS	16
9.1 PHONE USAGE	16
9.3 CALL MONITORING.....	17
SECTION 10: PHYSICAL SECURITY	17
10.1 PURPOSE	17
10.2 COMPUTING FACILITIES.....	17
10.3 OFFICE/WORKSTATION SECURITY	17
SECTION 11: REMOTE ACCESS AND MOBILE COMPUTING.....	17
11.1 REMOTE ACCESS.....	17
11.2 MOBILE COMPUTING	18
11.3 WIRELESS NETWORKS.....	19
SECTION 12: SECURITY INCIDENT PROCEDURES*	19
12.1 SECURITY INCIDENT DEFINITION.....	19
12.2 USER RESPONSE.....	20
SECTION 13: POLICY APPROVAL AND REVIEW	20

13.1 APPROVAL PROCESS	20
13.2 REVIEW POLICY	20
SECTION 14: APPEAL PROCESS.....	20
14 APPEAL PROCESS	20
APPENDIX 1: PERSONAL INFORMATION CLASSIFICATION.....	21
PERSONAL INFORMATION.....	21
APPENDIX 2: PROGRESSIVE DISCIPLINE.....	21
PROGRESSIVE DISCIPLINE POLICY	21

* Policy currently under development

Section 1: Overview and Purpose of this Policy

1.1 Overview

The University of Saint Francis has built an investment in computing resources over the course of its existence and has encouraged the University community to use these resources effectively in their work and studies. The computer facilities are a shared system made available to help foster an intellectual environment on the University Campus. The computer facilities promote a learning atmosphere for the University, create a sense of commitment to the local and global community and assist in preparation for living in a complex technological society. The network infrastructure, access to the Internet and online resources, powerful servers, and an increasing number of personal computers are assets in which we may take pride. Their value increases the more we take advantage of them. Using these resources in a responsible manner will protect this investment.

The University supports freedom of expression and an open environment for scholarly research. The contents of the University of Saint Francis computer systems must, however, comply with University policy, as well as local, state, and federal laws. This document is not meant to be a comprehensive list of what is allowed and not allowed, but a guide to ensure that computing resources are used ethically and responsibly within the university community. Effective security is a team effort involving the participation and support of every University employee and student and computer user. It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

This document should be considered a developing policy. Changes may be made as new questions and situations arise and shall reflect changes in policies and procedures.

1.2 Purpose

The purpose of this policy as a whole is:

- To protect and ensure the integrity of student and employee information
- To protect the university from litigation
- To follow government guidelines and applicable state and federal laws
- To develop procedures for the flow and access of data
- To define acceptable use of systems and university data
- To increase recovery capabilities in the event of a disaster

1.3 Definitions

Authorized User: a university employee, student, or other individual affiliated with the University who has been granted authorization to use a specific electronic resource.

Backup: To create a copy of critical files to minimize the loss of data in the event of a system failure.

University Technology Services: The University department responsible for the purchasing, management, and support of all computer, network, and telecommunications systems on campus.

Electronic Resource: Material in digital format which requires a computer device for use.

Email: Electronic Mail. Electronic messages sent from one person to another via electronic communication systems.

Employee: A person hired by the University of Saint Francis, whose primary role is to work for wages and salary.

Encryption: A security method used to transform data from its original form into a difficult to interpret format in order to prevent any but the intended recipient from reading that data.

Firewall: An access control device that acts as a barrier between two or more segments of a computer network, used to protect internal networks from unauthorized users or processes of other networks.

Internet: Global system of interconnected computers and computer networks. The computers and networks are owned and maintained separately by a host of organizations, government agencies, companies, and colleges and exist outside the USF network.

Intranet: A private network for communication and information that is only accessible to authorized users within the university.

Institutional Purposes: Broadly defined as legitimate items directly related to the mission of the University.

Logon: see "Username"

Mobile Computing: the ability to use technology in a non-fixed or non-static environment or location, via a portable computing or communication device such as a laptop, tablet, PDA, or cell phone.

Password: A string of characters known only to the user that serves as authentication of a person's identity. Passwords may be used to grant, or deny, access to information or resources. Access to systems or information is usually granted by a combination of Username and Password.

Personal Information: Information related to a person's private life or concerns, recorded in any form, by which individuals can be identified. Personal information can include: name, address, telephone number, race, ethnic origin, religious or political beliefs, bank account numbers, or social security numbers

Personal Files: Any type of record, document, or file that is of a personal nature and does not relate to the University or University business.

Privileged Information: Information confined to an exclusive or chosen group of users. Privileged information is not considered common knowledge, or has not been cleared for release to others outside the group.

Reasonable Efforts: Efforts based on known statements, events, or conditions. Reasonable efforts are defined as being within common sense, known best practices, or logical actions.

Remote Access: The ability to obtain access to an IT resource or the USF network from a location other than the physical campus of the University of Saint Francis, located at 2701 Spring Street, Fort Wayne, IN, or via a system or device not owned by the University of Saint Francis.

Security: Measures taken as to ensure a reliable computing platform free from the risk of loss.

Server: A system or computer program that provides information or services to other programs or devices.

Spam: Unauthorized and/or unsolicited mass electronic mailings.

Student: Person who is enrolled for study, as their primary role, at the University of Saint Francis.

TCP/IP: Transmission control protocol/Internet Protocol. This is a combined set of communication protocols that are used to perform data transfers between computers. These protocols are used to communicate over the Internet

User: Any individual who uses, logs in, attempt to use, or attempts to log into a system, whether by direct connection (modem or network) or across one or more networks.

UserID: see "Username"

Username: Also referred to as "logon" or "userID". A unique string of characters used to identify a specific user in a multi-user environment. Access to systems or information is usually granted by a combination of Username and Password.

Virtual Private Network (VPN): a private data network established within or across a public network that utilizes various security methods to transfer information.

Wireless Network: A network utilizing radio waves to transmit data as opposed to physical wired connections.

Common terms used to describe a wireless network include Wi-Fi, WLAN, or 802.11.

Webmaster: Person responsible for designing, managing, maintaining, and updating the website and web server.

Section 2: General Acceptable Use Policy

The Acceptable Use Policy is based on the University of Saint Francis' Complete Information Security Policies.

2.1 General Policies

University Technology Services computing facilities are available to all Saint Francis students, staff, and faculty and governed by the complete information security policies. The University of Saint Francis is committed to protecting USF employees, students, donors, and other stakeholders from illegal or damaging actions by individuals, either knowingly or unknowingly.

Computer systems, including but not limited to: computer equipment, software, storage media, network accounts, email, web browsing, and data residing on these systems are the property of the University of Saint Francis. These systems are to be used for institutional purposes in serving the interests of our University community.

The University strives to maintain an environment free of harassment and sensitive to the diversity of its students. The University, therefore, prohibits the use of computers and email in ways that are disruptive or offensive to others and/or harmful to morale.

University Technology Services strongly urges the backup of all personal files. Reasonable efforts will be made to mitigate losses or damage; however, individual users are ultimately responsible for backing up their personal files.

2.2 Availability

The University will make its computer facilities available with a minimum number of interruptions during normal business hours. Due to necessary maintenance the system may not be available at all times, however an attempt will be made to schedule such work at low usage times.

2.3. Right to Monitor

For security and network maintenance purposes, authorized individuals within the University of Saint Francis may monitor equipment, systems, and network traffic at any time, per established monitoring and audit procedures. For purposes of system maintenance all data and transmissions may be monitored, analyzed and viewed. The University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.4 Security

All users are expected to keep authorization codes secure. Passwords should not be shared with others and

should be changed frequently. Users are responsible for all actions taken using their password.

The University of Saint Francis cannot provide a system that allows users to store confidential information. For purposes of system maintenance networked files may be viewed. Users can assume networked information is free from censorship if the user complies with acceptable use and security policies. If at all possible, users will be notified if stored network information must be removed. Confidentiality will be maintained when Acceptable Use policies are followed. Users must be aware that electronic media is never 100% secure.

Stored information may be removed for reasons that include but are not limited to the following:

- The stored material was obtained illegally.
- The stored information endangers the integrity of the system.
- The user has used excessive storage system space.
- The stored information is in violation of local, state or federal laws.
- The stored information is inconsistent with the policies of The University of Saint Francis.

All media is susceptible to viruses and other types of malware. Therefore, users must make reasonable efforts to be sure their media is free from these types of destructive programs before using in any USF computing facility.

2.5 Legal Considerations

The University of Saint Francis is not responsible for any loss or damage to anyone's personal property including hardware, software or property of a mixed nature as a result of the use of the Saint Francis computer facilities. The University of Saint Francis resources are for institutional purposes only.

2.6 Enforcement

Users violating these policies will be subject to disciplinary action, up to and including dismissal, and will be reported to proper legal authorities as required by the situation.

At a minimum, access to network and computer resources will be revoked.

Section 3: Unacceptable Use

3.1 Unacceptable and prohibited activities

Unacceptable and prohibited activities include, but are not limited to, the following:

- Revealing your USF username and password to others (family members included)
- Using someone else's account
- Using USF systems for commercial purposes

- Using USF systems for unapproved political purposes
- Using the USF network as a means to gain unauthorized access to other systems/networks
- Use of illegal or unlicensed software
- Unauthorized network monitoring
- Copying and/or distributing commercial software without proper licensing
- Knowingly creating, executing, forwarding, or introducing any computer code designed to self-replicate, damage, or otherwise impede the performance of any computer, network device, or software.
- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulation.
- Using a University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace policies and laws.
- Making fraudulent offers of products, items, or services originating from a USF account.

Section 4: Data Management

4.1 Backup Policies

4.1.1 Scope

Backup procedures and policy intent is to cover all production server-based applications and data, allowing business resumption after the loss of a single server or an entire site. Only servers managed by University Technology Services are covered by this policy. Backup of material stored locally on end-user workstations is the responsibility of the user. For this reason, all users are strongly recommended to store copies of critical documents/files on network shares, and not on local drives.

4.1.2 Scheduling and Retention

A complete backup of all production servers will be made at least once per week, the most recent kept on-site for file recovery and the next most recent stored off-site. Between weekly backups, incremental backups will be used daily to ensure that a complete backup from the previous night is always available. Incremental sets will be maintained for a minimum of two weeks.

Backups shall normally be performed at night and on weekends. On occasion, particularly when a backup fails, University Technology Services may perform one or more backups during workdays. University Technology Services reserves the right to perform backups at any time, as deemed necessary by server administration.

This schedule means that files are only recoverable from the point in time at which they were backed up, in most cases the previous night. Files which did not exist at the time of the last backup are not recoverable. Applications and data can only be restored to the status they were in at the time the previous backup was completed.

Retention requirement associated with any document is determined by the content, not method of delivery or storage. Departments should be aware of documents that they are required to retain, and the method in which they must be stored.

4.1.3 Storage

All backup media shall be stored in a secure and environmentally controlled area. Removal from this secure area shall only take place for the purpose of using the media to perform a restoration, or moving backup sets to a designated off-site location. Access to this material shall be limited to Computing staff with a direct job responsibility requiring access.

4.1.4 Restoration

Servers requiring recovery from equipment failure or other catastrophic loss shall have the highest priority in restoration efforts. Requests for the restoration of individual files shall be handled as time allows.

4.1.5 Verification

Each backup job will be configured to verify the contents of the media after the backup is completed.

4.1.6. Servers residing off-campus

Hosted applications and servers that do not reside on campus may not fall within the University's ability to directly protect via in-house backup procedures. However, the University must take steps to ensure that business critical information is protected from disaster, regardless of physical location. Backup and restoration policies and procedures for all hosted applications will be documented and kept on file with the appropriate department. Before entering into an agreement for any hosted application, it must be determined that backup procedures are adequate for the type of service hosted.

4.2 Storage of Copyrighted Material on USF Machines

The purpose of this policy is to limit the University's liability in regards to copyright infringement.

USF retains all ownership of its computer systems, networks, and the data they contain. Copyrighted material that is not legally licensed to the University should not be stored on USF-owned machines without express written consent of the copyright owner. Copyrighted material includes, but it not limited to: software, MP3 files, movies, multimedia, and electronic books.

4.3 Information Handling

4.3.1 Care and Handling of External Information

External information is defined as any information collected, bought, or given by a source outside the university. Many times this information comes with copyright or confidentiality agreements that dictate how the information is used. The university will adhere to any such agreements accompanying this information

4.3.2 Care and Handling of Internal Information

Internal Information is defined as any information collected and maintained by the University. The University of Saint Francis is the owner of this information. Any data managers of this information will be designated as needed.

The Jenzabar administrative software package is an integrated, inter-departmental database where much of the University's information is stored. Access to the Jenzabar system, and the information it contains, is authorized by the area Vice President of the maintained data. Requests for information (reports, labels, etc) or access to the Jenzabar module must be verified with the manager of the module. Module Managers are the designated "experts" of each individual module. Each Module Manager operates under the direction of an area Vice President or similarly titled individual.

Module managers will be trained in the type of information that can be disclosed to others. It is the responsibility of the module manager to verify that the information requested will be used in accordance with FERPA guidelines and University policy.

4.3.3 FERPA:

The Family Educational Rights and Privacy Act (FERPA) is a federal law protecting the privacy of student education records. USF considers student records private information, belonging to the student. The University must have written permission from the eligible student in order to release any information from a student's record. The Registrar's office is responsible for developing, maintaining, and educating the USF community regarding FERPA compliance policies at USF.

4.3.4 HIPAA:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) authorized the development of security and privacy standards to protect healthcare information that is stored electronically. These standards cover processing, storage, and transmission of health information to prevent unauthorized or inadvertent use or disclosure of an individual's health information. The Human Resources department is responsible for developing, maintaining, and educating the USF community regarding HIPAA compliance policies at USF.

4.3.5 Data Misuse

Data misuse is defined as using university-owned data (either unintentionally or deliberately) in a manner inconsistent with university policy, or federal, state, or local laws. Examples of data misuse include:

- Obtaining or attempting to obtain access to data not within the scope of one's University job

responsibilities

- Downloading or exporting centrally held information into non-approved databases or personally owned equipment
- Using University data for personal benefit
- Releasing information in an inappropriate manner
- Using information inaccurately, conflicting with published, sanctioned University information and/or statistics

Section 5: Access Policies

5.1 Username and Password Policies

5.1.1 Employee Responsibilities:

Employees will be assigned a USF account that allows use of certain USF computing resources. Accounts will be designated by a username (User ID) and protected by a confidential password known only to the employee.

Employees are required to enter their username and password in order to use USF computing resources.

If a password is entered incorrectly three times in a row, the account will be locked and the user will not be able to log on until the lockout expires, or it is unlocked by a password administrator, normally the Help Desk.

Passwords must be changed as determined at the domain level. Users will be reminded to change their password 14 days in advance. If users do not change their password by the end of this time, the account will be locked and they will not be able to log in until a password administrator unlocks it.

Employees should avoid writing their password. If they must do so, they are responsible for ensuring that no one else has access to the written password. Users shall never write both the username and password together.

Users are responsible for protecting user identification and passwords. If it is believed that someone else knows a user's password, or is using an account other than their own, the password should immediately be changed and University Technology Services notified.

Users **must not** share their password with anyone, or log in and allow another user to work using their personal User ID and password. If there is need to grant access to an outside user, that user must follow appropriate procedures to apply for access.

If a password is forgotten or needs to be reset, the request must be made in person at a designated password reset location. Passwords will not be sent via mail or email, or given to others.

5.1.2 Password Requirements:

A network password is the key to access most systems on campus. All USF employees and users are expected to keep ALL system passwords private. Our security policy requires the following:

- It must have a minimum of eight (8) characters
- It must not contain all or part of the user's account name
- It must contain characters from at least three of the following four categories:
 1. English Uppercase characters (A through Z)
 2. English Lowercase characters (a through z)
 3. At least one number (0-9)
 4. Non-alphanumeric characters (example: !, \$, #, %, ^)

In addition, we strongly recommend:

- It should contain both lower and upper case letters (passwords are case-sensitive)
- It should contain *at least* one special character (@, #, {, }, \$, %, etc.
- Never use a person's name or any word that could be found in the dictionary. Breaking up words with special characters or numbers is an easy way to avoid this.
- Do not use the same passwords for work as you do for personal use

5.2 Supervisor responsibilities

Managers and supervisors are responsible for notifying University Technology Services when (or before) an employee leaves the university or transfers to another department so that access can be revoked. Terminations **must** be reported to University Technology Services immediately upon learning of the termination.

5.3 Guest and Special Access

Occasionally it may be necessary to grant access to computing resources to individuals other than employees of the University. Examples of such individuals are consultants, review board members, and volunteers. Employees must never give out their passwords to others. If access is needed by external individuals, it should be requested from University Technology Services

University Technology Services reserves the right to refuse access to any such individual if access is inappropriate or violates information security policies or any applicable laws.

5.4 Access Audits

University Technology Services may routinely audit access to university computing resources and reserves the right to temporarily disable questionable access. Department heads are responsible for periodically reviewing

access to their information and must notify University Technology Services if access should be revoked or levels changed.

Section 6: Internet and Intranet Policies

6.1 Internet Security Policy

Internet Users shall be aware that as they access Internet resources, they will be associated with the University through the mechanisms of the TCP/IP protocols. Therefore, users shall access resources in accordance with their job description.

While online, users shall be cautious as to what they disclose to others. Users shall remember that email and internet transmissions are not private information. Anything sent could possibly be read by individuals other than the intended recipient. Users shall not transmit any information that may be damaging to the organization or themselves. Privileged and private information, as covered in other university policies, shall not be transmitted without proper precautions. Users should exercise similar care when transmitting personal data.

6.2 Intranet

6.2.1 Intranet content

Content of the USF Intranet is restricted to official university business. Posting on the campus Intranet is open to all departments who have intra-departmental communication needs. Request to participate must be submitted by the appropriate department head. Submission of a request implies department head's accountability for all content, misuse and misinformation posted on their behalf. It is also the responsibility of the department head to ensure the content is kept current.

6.2.2 Intranet access

Access to the USF Intranet is granted to all employees via their network username and password. Due to the potentially confidential nature of content on the USF Intranet, students will not be granted access.

6.3 www.sf.edu Website Policies

The www.sf.edu website is the University of Saint Francis' web identity to the entire world. For this reason, content placed on this website must reflect the image and values of the university.

Section 7: Email Policies

The purpose of this policy is to outline the security of email and state University and User responsibilities in regard to email systems and content.

7.1 Email definitions and purpose

The campus faculty and staff e-mail system is provided as a means of communication of USF-related business. Electronic data (including backup copies) stored, maintained, or using USF equipment is the property of USF, not the user. Electronic messages should follow the same standards expected in written communication, and should adhere to the Information Security Policies as well as any other applicable university policy.

Email is the equivalent of an Internet "postcard", and cannot be guaranteed private. Users should be aware that emails could be received, forwarded, intercepted, printed, or saved by people other than the intended recipient. The University reserves the right to monitor content and usage for maintenance, operational, auditing, security, or investigation-related reasons.

7.2 Content Scanning

The University shall be allowed to scan the content of every email message that passes through its servers based on a predetermined set of criteria. If the message does not pass the criteria, it will not be delivered to the user. Email administrators shall have procedures in place for determining content scanning criteria.

7.3 Email Virus Protection

University Technology Services staff members are responsible for creating and maintaining procedures for preventing and handling infected email messages. Email that has been found to be infected with a virus, worm, Trojan horse, or contains another executable item that could pose a threat to security will not be delivered to the user. Known Infected email will be removed from the delivery system. If a virus outbreak is suspected, email service may be interrupted without notice.

7.5 Size Limits

Mailbox sizes will be limited as appropriate based on current mail server storage capacity. Email messages sent to and from users shall not exceed limits set by the email administrator.

7.6 Email Backup

The email system is backed up by University Technology Services to the extent of allowing email service resumption after the loss of a single server or an entire site. Individual messages within the email system are not backed up by University Technology Services.

Section 8: Software Compliance

8.1 Software Policy Purpose

The University of Saint Francis ("USF") licenses the use of computer software from a variety of outside

companies. The University does not own this software or its related documentation. Unless expressly authorized to do so, the University has no right to make copies of the software except for backup or archival purposes. The purpose of this policy is to prevent copyright infringement and to protect the integrity of the USF computer environment from viruses. This anti-piracy statement must be reviewed by all users prior to gaining access to computer resources, and constitutes an employee agreement.

8.2 Software Guidelines

8.2.1 General Statement of Policy

It is the policy of the University of Saint Francis to respect all computer software copyrights and to adhere to the terms of all software licenses to which USF is a party. The University shall take all steps necessary to prohibit users from duplicating any licensed software or related documentation for use either on USF premises or elsewhere, unless expressly authorized to do so by the licensor. Unauthorized duplication of software may subject users and the University to both civil and criminal penalties under the United States Copyright Act.

In accordance with US copyright laws, USF must not permit any employee to use software in any manner inconsistent with the applicable license agreement. This includes giving or receiving software or fonts from students, colleagues, or others.

8.2.2 Acquisition of Software

All software acquired by the University must be purchased through University Technology Services. Software may not be purchased using business credit cards, petty cash, travel, or entertainment budgets. Software acquisition channels are restricted to ensure that USF has a complete record of all software that has been purchased for USF computers and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

8.2.3 Registration of Software

When USF receives the software, University Technology Services must receive the software to complete registration and inventory requirements before installation. Software must be registered in the name of University of Saint Francis and the department in which it will be used. Due to personnel turnover, software will never be registered in the name of an individual user. University Technology Services maintains a database of all software, and will keep a library of software licenses. The database must contain: a) the title and publisher of the software; b) the date and source of software acquisition; c) the location of each installation as well as the serial number of the hardware on which each copy of the software is installed; d) the existence and location of back-up copies; and e) the software product's serial number

8.2.4 Installation of Software

After the registration requirements above have been met, the software shall be installed by a member of University Technology Services staff. Once installed, the original media shall be kept in a storage area maintained by University Technology Services. User manuals, if provided, shall either reside with the user or reside with University Technology Services (dependent on the situation).

8.2.5 Client/Server Applications

With regard to client/server and network applications, USF employees shall use the software only in accordance with license agreements. University Technology Services will only install client applications as expressly permitted by its associated license agreement.

8.2.6 Home Computers

USF computers are University-owned assets and must be kept both software-legal and virus free. Only software purchased through the procedures outlined above may be used on USF machines. Users are not permitted to bring software from home and load it onto USF computers. Generally, USF-owned software cannot be taken home and loaded on a user's home computer if it also resides on a USF computer. However, some software packages allow home use in some circumstances. If a user needs to use software at home, he/she should consult with University Technology Services to determine appropriate licensing.

8.2.7 Shareware

Shareware software is copyrighted software that is distributed via the Internet. It is the policy of USF to pay shareware authors the fee they specify for use of their products. Under this policy, acquisition and registration of shareware products will be handled the same as for commercial software products.

8.3 Quarterly Audits

University Technology Services will conduct a quarterly audit of all USF PCs and servers, including portables, to ensure that USF is in compliance with all software licenses. University Technology Services reserves the right to also conduct surprise audits. Audits will be conducted using an auditing software product. The full cooperation of all users is required during audits. If unauthorized software is discovered, it will be removed from the user's system and the user may be documented as in violation of the USF security policy.

8.4 Penalties and Reprimands

According to the US Copyright Act, illegal reproduction of software is subject to civil damages of as much as US\$150,000 per title infringed, and criminal penalties, including fines of as much as US\$250,000 and imprisonment of up to five years. Any USF computer user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances. Such discipline may include termination of employment. The University of Saint Francis does not condone the illegal duplication of software and will not tolerate it under any circumstances.

Section 9: Telecommunications

9.1 Phone Usage

Employees will be given phones and voicemail as necessary for conducting University business.

9.3 Call Monitoring

The University of Saint Francis reserves the right to monitor phone usage.

Section 10: Physical Security

10.1 Purpose

The purpose of this policy is to outline the minimum physical security expected for Computing facilities and all computing equipment.

10.2 Computing Facilities

Computing facilities shall be of sufficient size with multiple exits. The areas used for servers shall have sufficient environmental controls that include temperature and humidity controls.

Sufficient access controls shall be installed to prevent unauthorized physical access to computing facilities.

10.3 Office/Workstation Security

All users shall be responsible for maintaining the security of their assigned workstation. Required security provisions include locking or logging off workstations when not in use, and preventing unauthorized physical access to unattended systems.

Section 11: Remote Access and Mobile Computing

11.1 Remote Access

11.1.1 Purpose:

University data that is processed or stored on systems outside of the University premises or via systems not owned by the university are generally more vulnerable to being lost, compromised, or corrupted. The purpose of this policy is to provide guidelines for Remote Access or Virtual Private Network (VPN) connections to the University of Saint Francis network or information technology (IT) resources.

11.1.2 Scope and Remote Access Terms of Use:

This policy applies to all University technology users utilizing any type of remote access to gain entry to the USF network or access to USF information technology resources.

Approved USF employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of remote access and VPN's. Use of remote access services normally requires an existing internet connection be available prior to use. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying associated fees.

11.1.3 Available Resources:

Users should be aware that remote access to the USF network does not guarantee access to identical resources as are available when working on the physical USF campus. Various factors, including current system limitations, applicable license agreements, and required security provisions will determine which resources are accessible via a remote connection, as well as the methods by which these resources are accessed. University Technology Services (UTS) is responsible for determining an IT resource's suitability for remote access.

11.1.4 Additional Provisions:

1. It is the responsibility of users with remote access privileges to ensure that unauthorized users are not allowed access to USF internal networks and resources.
2. Remote access use is to be controlled using password authentication. Passwords for remote access shall not be saved on end-user computers or devices.
3. Remote access services, including but not limited to, gateways and servers will be set up and managed by University Technology Services. Only UTS-approved remote access clients and services may be used.
4. All computers connected to USF internal networks via remote access must use the most up-to-date UTS-approved anti-virus software and security patches; this includes computers that may be personally owned.
5. By using remote access technology with personal equipment, users must understand that their machines are, in effect, an extension of USF's network, and as such are subject to the same rules and regulations that apply to university-owned equipment, i.e., their machines must be configured to comply with USF Information Technology Security Policies.
6. It is the responsibility of the user to be aware of specific information handling requirements when working with university data via a remote connection.

11.2 Mobile Computing

11.2.1 Purpose

The purpose of this policy is to provide guidelines for ensuring greater security between USF and all users with access to USF systems and information using mobile computing devices. This applies to any mobile computing device connected to USF Information Technology resources, used to process or store University data, or conduct University business. Mobile devices include various types of equipment such as PDAs, SmartPhones, notebook or tablet computers.

11.2.2 Security Provisions

It is highly likely that mobile devices used for university business, or even "synched" with a USF system contain confidential information in the form of email correspondence, documents, or other files. It is the responsibility of the user to ensure that information stored on the mobile device is protected as required by applicable state and federal laws such as FERPA and HIPAA. Users must meet the following security provisions before the device is used to process or store University data, or connect to USF information technology resources.

1. Password Policies: All mobile devices must be secured using a logon or power-on password.
2. Virus Protection: UTS-approved virus protection must be installed and up-to-date on any device where such utility is commonly available.
3. Required system patches and updates: Mobile device users must ensure that devices are up-to-date with required software patches and updates, for example, Windows Updates or Palm software updates.
4. Data ownership: Users must be aware that all information synched from the USF network is the property of the University and not the individual.

11.2.3 PDAs and SmartPhones – Additional Provision

Personal Digital Assistants (PDAs) and SmartPhones are not considered secure computing devices. Under no circumstances should confidential and highly sensitive information be stored on a device of this type. Protected information of any university student or constituent, such as personal data including SSN, must NEVER be stored on a PDA or SmartPhone. Failure to follow this security provision will result in disciplinary action.

11.3 Wireless Networks

11.3.1 Purpose

As wireless networks are often utilized with remote access and mobile computing, the purpose of this policy is to provide guidelines for ensuring greater security to users using this method of network connectivity.

11.3.2 Security Provisions

Wireless networks are inherently insecure. In any wireless network, the transmission over public airspace always poses a risk of interception and capture, regardless of the methods of encryption or security. Because of the inherent security risks when using a wireless system, users assume responsibility for any data transmitted via this connection. All users are expected to exercise caution when using a wireless network.

When using a wireless network to transmit university data (including accessing University email servers), users must be aware of the following network types and adhere to the security provisions:

1. **Unknown Networks:** Users should never utilize wireless network of an unknown source to transmit university data. Unknown networks include those wireless networks that you have not been given specific permission or instructions for connection, but rather have “discovered” via wireless detection built into a mobile device. These types of networks are commonly set up with the specific purpose of attracting unsuspecting users and capturing any information transmitted.
2. **Encrypted networks:** Encrypted networks are those that require some type of authentication and encryption method prior to data transmission. Whenever possible, an encrypted network should be used. Encryption methods should match the requirements type of data being transmitted. For example, personal information should NEVER be transmitted via a wireless network without strong encryption in place.
3. **Open Networks:** Open networks are common “free Wi-Fi” connections and often do not require any type of login or authentication in order to use. Users are strongly encouraged to NEVER utilize an open network for transmitting confidential or sensitive university data.

Section 12: Security Incident Procedures

Note: Policy section currently under development.

12.1 Security Incident Definition

A security incident is defined as any act that violates an explicit security policy. Violations may include events having actual or potential adverse effects which compromise an aspect of computer, network or user resources, including but not limited to: loss of confidentiality of information; a compromise of the integrity of information; misuse of service, systems or information; damage to systems and damage or loss of property or information.

12.2 User Response

University Technology Services should immediately be notified with the following information:

- Date and time of incident
- Type of incident and any other pertinent details that would assist in verifying incident
- A statement describing the impact on users, department or the network including the number of users/departments affected.
- Contact information of submitter

Additional incident response requirements currently under development.

Section 13: Policy Approval and Review

13.1 Approval Process

The University of Saint Francis Security Policy must be reviewed and approved annually by the Director of Technology Security and Compliance, Executive Director of University Technology Services, Risk Management Committee, and the USF Leadership Team.

13.2 Review Policy

The University of Saint Francis Security Policy shall be reviewed and updated as deemed necessary by the Director of Technology Security and Compliance, at least once annually.

Section 14: Appeal Process

14 Appeal Process

Decisions regarding information technology security at USF are made based on current information technology law, and common best practices. Employees who may disagree with decisions based on this policy should follow established problem resolution/appeal procedures as outlined in applicable employment handbooks.

Appendix 1: Personal Information Classification

Personal Information

Under Indiana Code 24-4.9, "*Personal Information*" is defined as follows:

"*Personal information*" means:

- (1) a Social Security number that is not encrypted or redacted; or
- (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:
 - (A) A driver's license number.
 - (B) A state identification card number.

Source: House Enrolled Act No. 1101 (<http://www.in.gov/legislative/bills/2006/HE/HE1101.1.html>)

Appendix 2: Progressive Discipline

Consequences for all Information Technology Security Policy violations shall follow the progressive discipline policy as outlined in the USF Employee Handbook.

Progressive Discipline Policy

The best disciplinary measure is the one that does not have to be enforced and comes from good leadership and fair supervision at all employment levels. University of Saint Francis' own best interest lies in ensuring fair treatment of all employees and in making certain that disciplinary actions are prompt, uniform and impartial. The major purpose of any disciplinary action is to correct the problem, prevent recurrence, and prepare the employee for satisfactory service in the future.

To ensure orderly operations and provide the best possible work environment, the university expects employees to follow rules of conduct that will protect the interests and safety of all employees and the university. Employees are required to conduct themselves in a manner according to the Mission Statement of the University of Saint Francis.

Although employment with University of Saint Francis is based on mutual consent and both the employee and the university have the right to terminate employment at will, with or without cause or advance notice, the university may use progressive discipline at its discretion. **Disciplinary action may call for any of four steps – verbal warning, written warning, suspension with or without pay, or termination of employment – depending on the severity of the problem and the number of occurrences. There may be circumstances**

when one or more steps are bypassed.

Progressive discipline means that, with respect to most disciplinary problems, these steps will normally be followed: a first offense may call for a verbal warning; a next offense may be followed by a written warning; another offense may lead to a second written warning or suspension; and, still another offense may then lead to a third written warning. Upon receiving three written warnings within a twelve-month period for a violation of university policy, the employee is subject to termination of employment. If more than 12 months have passed since the last disciplinary action, the process will normally start over.

University of Saint Francis recognizes that there are certain types of employee problems that are serious enough to justify either a suspension, or, in extreme situations, termination of employment without going through the usual progressive disciplinary steps. While it is impossible to list every type of behavior that may be deemed a serious offense, the following are examples that may result in disciplinary action up to and including termination of employment:

- Theft or inappropriate removal or possession of property.
- Falsification on application or of time keeping records
- Working under the influence of alcohol or illegal drugs
- Possession, distribution, sale, transfer, or use of alcohol or illegal drugs in the workplace, while on duty, or while operating employer-owned vehicles or equipment.

Other behaviors that are deemed inappropriate and are subject to the disciplinary procedure, up to and including termination of employment, are defined as, but not necessarily limited to, the following:

- Divulging information that the university considers confidential
- Irregular attendance or excessive absenteeism
- Failure to abide by safety rules
- Neglect of duty
- Insubordination
- Dishonesty
- Disorderly conduct
- Willful destruction of university property
- Habits or state of health dangerous to the worker, coworkers, or the students
- Abuse of business travel policy and/or any other policy of the university

Any behavior or conduct, whether in written, verbal, or non-verbal form, which is not in accordance with the Mission Statement and the Franciscan Values of the University of Saint Francis.