

Saint Louis University

Information Security Policies and Guidance Manual

Adopted: December 21, 2004

Table of Contents

- I. [Goals and Objectives](#)
- II. [Policy Scope](#)

- III. [Background](#)

- IV. [Information Security Management](#)
 - A. [Information Security Committee](#)
 - B. [The Data Steward](#)
 - C. [Security Review Committee and Processes; Application Service Provider Review](#)
 - D. [Vulnerability Oversight Committee](#)
 - E. [Incident Response Team](#)

- V. [Network Management Policy](#)
 - A. [Host Configuration and Logging Requirements](#)
 - B. [User Access and Authentication Requirements](#)
 - C. [Use of Non-University-Owned Equipment](#)
 - D. [Use of Wireless Devices](#)

- VI. [Restrictions on Use of Social Security Number](#)

- VII. [Requirements for Data Encryption](#)

- VIII. [Virus and Malicious Code Prevention](#)

- IX. [Technology Equipment Disposal Requirements](#)

- X. [Physical Security Requirements](#)

- XI. [Reporting Network Abuse or Security Violations](#)

- XII. [Education/Training](#)

- XII. [Sanctions for Policy Violations](#)

I. Goals and Objectives

The primary goal of the University's Information Security policies is to protect and secure sensitive and/or regulated University information. In order to accomplish this goal, the University has set forth a policy framework that:

- Employs University-wide participation
- Establishes the role of informed representative (data steward) for the use and protection of specific sensitive and/or regulated information
- Establishes requirements for security review of electronic business processes
- Ensures understanding of business and academic needs
- Provides feedback mechanisms to strengthen the policy framework
- Encourages a culture of participation, information sharing, support, and education

The University community is the key to the success of these policies. Through the participation of its faculty, staff, and students, the University can continually work to protect and secure sensitive information within its systems.

II. Policy Scope

These policies, requirements, and procedures, as well as guidelines and standards that derive from them, apply to all University employees, departments, and divisions, and all University information technology systems. These policies supersede all previous Information Technology policies.

III. Background

Efforts to develop the policies contained in this handbook were initially prompted by the University's need to comply with the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA). The University's Information Security Committee (ISC) was formed in 2002 and charged by the Provost and the University's HIPAA Oversight Committee to develop the University's approach to compliance with the HIPAA Security Rule. The ISC was comprised of approximately 25 individuals from across the University, and included faculty, staff, and student representatives.

During the course of the ISC's work, it became clear that the University required a broader approach to information security policy than was mandated by HIPAA. A number of other regulations and concerns, including Gramm-Leach-Bliley (GLB), the Family Educational Rights and Privacy Act (FERPA), and the use of Social Security numbers also mandated a more comprehensive approach to information security. These regulations and concerns, as well as continuing national and international incidents involving data compromise, resulted in a broadening of the ISC's policy development scope to include security for all types of regulated or sensitive information. This included information in non-electronic formats as well.

It was a challenge to develop broad-based policies dealing with specific types of information across a complicated organization. In response to this challenge, the committee focused on the development of a new “participatory” policy framework designed to provide the direction and guidance needed to protect sensitive University information, while being as responsive as possible to administrative, research, and academic needs.

The framework for these policies and requirements can be found in the first policy contained in this manual—the Information Security Management Policy. Within this framework, some responsibilities are centralized and some are distributed to stakeholders. This structure is meant to achieve high levels of participation as well as opportunities for input across the University community. It is also designed to bring together University stakeholders to share strategies for information security, and to ensure that policies and procedures developed to address information security are working in practice.

It is the intent of the Information Security Committee to continually evaluate policy and procedure implementation in concert with the Provost, the Vice President of Information Technology Services, and the General Counsel, and to make adjustments where needed in order to more fully ensure the security of information in the University’s possession.

IV. Information Security Management

This policy establishes an information security management structure that includes broad representation from within the University community to develop and implement policies, procedures, and standards regarding information security, and to comply with applicable laws and regulations. Broad University representation encourages greater understanding of policies, rules, and regulations, as well as timely, effective policy development and implementation.

A primary goal of this management structure is the creation of a culture that encourages participation, information sharing, and education. This culture should enhance the University’s ability to protect confidential information as well as its compliance with laws and regulations centering on stewardship of information.

Generally, the management structure is focused on collaboration between information technology experts and information users across the University community. It relies on technical expertise as well as business process expertise; therefore, the structure outlines a number of roles within the technology and technology user communities.

The management structure also establishes an important role within the technology user community entitled “**Data Steward.**” This role is vital for representing business processes, and for education regarding secure information handling throughout the University community. This includes the handling of information verbally, on paper, and electronically.

The information security management structure outlined in this policy is comprised of three groups: the Information Security Committee (ISC), including the role of the Data

Steward; the Security Review Committee (SRC); and the Vulnerability Oversight Committee (VOC).

A. The Information Security Committee

The Information Security Committee is responsible for developing information security policies in accord with applicable laws and regulations, overseeing policy implementation, providing oversight for policy compliance; and serving as arbiter in issues regarding information security and technology needs. The ISC reports to the Provost, coordinates with the Vulnerability Oversight Committee, and oversees the Security Review Committee.

Committee Membership

At least five representatives from non-ITS departments must serve on the ISC at any given time. The Provost will make appointments to the ISC.

1. ISC Chair – This position is appointed by the Provost, and held by a high-ranking University administrator in a non-ITS department.
2. ISC Associate Chair – University Information Security Officer
3. ISC Associate Chair – University Privacy Officer

Other members:

4. Vice President, Information Technology Services.
5. *Data Steward* for patient health information (this includes information affected by Health Insurance Portability and Accountability Act--HIPAA--regulations)
6. *Data Steward* for student records (this includes information affected by Family Educational Rights and Privacy Act--FERPA--regulations),
7. *Data Steward* for information involving University financial transactions (this includes information affected by Gramm Leach Bliley--GLB--regulations),
8. *Data Steward* for clinical practice concerns,
9. *Data Steward* for electronic health records,
10. At least one faculty representative,
11. At least one staff representative,
12. Other representation to address needs for specific expertise as issues arise.

Committee Responsibilities

1. Develop and review Saint Louis University information security policies.
2. Appoint ad hoc committees to develop procedures and standards deriving from information security policies. The ISC ensures that

these committees work closely with the Vulnerability Oversight Committee in the development of all procedures and standards.

3. Review and approve all proposed changes that could not be resolved in the Security Review Committee.
4. Ensure continuing risk assessment with the assistance of the Vulnerability Oversight Committee, the Security Review Committee, ITS, and outside consultants, if necessary.
5. Conduct or elicit both internal and external audits of systems and practices to ensure security of the networks, information, and soundness of policy and procedures.
6. Notify Provost and Vice President, Information Technology Services regarding issues of non-compliance.

Committee Processes and Rulings

It is expected that each member will participate in all committee functions. If a member is unable to attend a meeting, he or she must appoint an alternate member to represent his/her area. In no case, however, will the alternate member be allowed to vote on behalf of the committee member. If a member of the committee cannot fully participate in the functions of the ISC, the chair will notify the Provost, who may appoint another representative.

All committee rulings shall be decided by consensus of the total current membership. In the event of a split decision or dissenting opinion(s), the committee will present the Provost with synopses of the dissenting opinion(s), and the Provost will make a final determination.

B. The Data Steward

University information is classified as either **public** or **confidential**. Public information refers to the type of information that can be freely shared with others, either internally or externally. Confidential information refers to the type of information that must be protected and may not be shared freely. The protection of confidential information is of the utmost importance. Therefore, access to University confidential information is granted on a “need-to-know” basis only.

Because there are so many types of confidential, protected information stored and used within the University, specific procedures for the handling of each type of protected information must be developed and shared with all University employees dealing with this protected information in their work. To assist in the management and protection of confidential, protected University information, a representative for each protected type of data is appointed by the Provost. These representatives are referred to as “**Data Stewards**” and have broad responsibility for their respective data types. Data Stewards

serve on the University's Information Security Committee to ensure effective policy and procedure development and implementation concerning specially regulated types of University data.

Typically, the role of Data Steward will be filled by a high-level participant in the daily handling of specific types of sensitive data (e.g. patient health information). Data Stewards will work to ensure that all policies, procedures, and standards regarding the use of sensitive University information are effectively implemented in their respective work areas. Data Stewards will also work to ensure ISC understanding of users' needs.

Data Steward Responsibilities:

1. Develop data handling plans and procedures for review by the Information Security Committee. The ISC can provide additional advice or guidance in the protection of confidential information.
2. Ensure that all employees who handle confidential information are trained in proper information handling procedures. Data stewards will have the authority to enlist appropriate assistance from departments that deal with confidential data in order to accomplish goals related to education, reporting, and overall compliance.
3. Serve on the University's Information Security Committee.

C. Security Review Committee

The Security Review Committee (SRC) is charged with review and approval of any and all changes to the University's technology infrastructure that impact security. The SRC ensures that proposed *Computing and Network Changes* are reviewed in a timely manner to minimize disruption to academic, research, clinical, and business operations; provides an open forum to discuss ideas and concerns; and ensures proposed changes comply with University policies, procedures, and standards.

Committee membership

1. Chair – Appointed by the Vice President of Information Technology Services, the chair will manage the membership of the Committee.
2. Coordinator – an IT network representative.
3. Additional ITS representations from the following areas:
 - Desktop
 - Infrastructure
 - Security
 - Privacy

Support
Administrative Information Systems

4. Ad hoc faculty and/or student representation dependent on the specific request submitted for committee review. The Vice President of Information Technology Services, in concert with the Provost, will be responsible for requesting faculty and/or student participation in specific committee reviews.

Committee Responsibilities

1. Review and approve all computing and network change proposals for compliance with existing University policies, procedures, and standards, as well as security issues that might occur in the context of the proposed change.
2. Review and approval for the potential use of an “Application Service Provider” prior to the arrangement of any contractual commitment or purchase of equipment, software, and/or services. The review will ensure compliance with existing University policies, procedures, and standards, as well as security issues that might occur in the context of the proposed change. Prior to such review, the appropriate vice president or dean must provide approval to explore ASP services. Additionally, General Counsel’s office or his/her designee must review and approve any agreement or contract that would engage an ASP prior to such a commitment being made. As the University’s security standards change over time, the ASP is expected to comply with such changes, given reasonable notice.
3. Coordinate with those who propose changes to ensure the most effective security for any change and a thorough understanding of any security concerns.
4. Report security concerns to the ISC, and recommend appropriate remediation measures.

Committee Processes and Rulings

It is expected that each member will participate in all committee functions. If a member is unable to attend a meeting, he or she must appoint an alternate member to represent his/her area. In no case, however, will the alternate member be allowed to vote on behalf of the committee member. If a member of the committee cannot fully participate in the functions of the SRC, the chair will notify the Vice President, Information Technology Services, who may appoint another representative.

All committee rulings must be decided by consensus of the total current membership. In the event of a split decision or dissenting opinion(s), the committee will present the Information Security Committee with synopses of the dissenting opinion(s), and the ISC will make a determination.

The Security Review will serve as a component of the Project Management Process defined by the Division of Information Technology Services. ITS will employ a “triage” process for all requests for assistance from the technology user community that will automatically prompt a security review by the committee for any request that poses a risk to information security. ITS will develop and keep updated a list of changes, projects, and/or requests for which a security review must be employed and will make this list available widely as part of its project management process description. ITS will also ensure tracking and documentation of the project management process, that will include complete documentation of the security review.

D. Vulnerability Oversight Committee

The Vulnerability Oversight Committee (VOC) is charged with security maintenance through risk assessment, prevention, detection, and response to information security-related incidents. The VOC reports to the Vice President, Information Technology Services.

The VOC works with the University community to identify security risks and to establish disaster recovery plans in order to minimize the risk of loss of information or data security, whether the information is public or confidential. The preparation of disaster recovery plans is an important component in preventing loss or minimizing loss should a disaster occur.

Committee membership

The Vice President, Information Technology Services, appoints the chair of the VOC from its membership. Members include:

1. University Information Security Officer
2. University Network Security Analyst
3. University Compliance representative
4. University Privacy Officer
5. Risk Management representative
6. Client-server architecture representative
7. Application database representative

Disaster Plan development

All departments and/or divisions that are responsible for maintaining network or server operations must develop and maintain disaster recovery plans for necessary

business and processing operations in order to protect University information and business activities. Likewise, all University departments and/or divisions must develop disaster recovery plans for information stored in physical form. These plans must address the full range of resources including, but not limited to, data processing, data communications links, personnel, power supply, desktop computers, and the recovery of physically stored information.

The Vice President of Information Technology Services and his/her designees are responsible for identifying, protecting, and planning the recovery of all University communications, hardware, and software assets deemed critical to the continued operation of the University's central administrative, academic, and supplemental systems.

All departments and/or divisions that are responsible for maintaining network or server operations must submit their respective disaster recovery plans to the Vulnerability Oversight Committee for review and approval. The VOC will work with administrators to ensure appropriate development and periodic review of each plan.

Committee responsibilities

1. Establish methods and procedures to prevent and detect security breaches in the University's technology infrastructure, while balancing the need to maintain user confidentiality and privacy.
2. Conduct vulnerability analyses, including *inter-incident analyses*, consult with appropriate individuals, and advise the Vice President, Information Technology Services, regarding prevention and detection needs.
3. Review disaster recovery plans.
4. Oversee the University's **Incident Response Team (IRT)**, which is responsible for undertaking necessary actions, up to and including disconnection, to protect the University's technology infrastructure in a security emergency.

E. Incident Response Team

The Incident Response Team is comprised of representatives from the following departments. These individuals are called on an as-needed basis, i.e. dependent on the nature of a security breach, in the case of a security incident.

1. ITS Helpdesk
2. ITS Networking
3. ITS System Administrators

4. ITS Workstation Support
5. ITS Application Support
6. University Public Safety
7. Student Life
8. Human Resources
9. Department(s) involved in the incident
10. ITS Operations
11. Any other need-to-know departments

The Incident Response Team is required to follow a specific set of procedures in order to preserve evidence of a security breach, and to provide complete documentation of any security incident, including an *intra-incident analysis*, to the Vulnerability Oversight Committee. These procedures will be developed by the Vulnerability Oversight Committee, in coordination with appropriate members of the Incident Response Team.

V. Network Management

Configuration, maintenance, and documentation of the University's computing network are the responsibility of the Vice President of Information Technology Services or his/her designee(s). For that reason, Information Technology Services (ITS) must be provided administrative access at the highest level to all electronic and physical components of the University's network and must adhere to the following requirements:

1. All hosts (clients and servers) must be configured to standards established by ITS. ITS will make these standards available to non-ITS computing administrators on an as-needed basis.
2. Any proposed change to the University's computing network must be reviewed and approved for security concerns by the Security Review Committee prior to implementation and/or purchase of related equipment and/or software. Changes to the University's computing network include the following:
 - a. Modifications or extensions to the network transport layer (the wire and cabling infrastructure);
 - b. Redeployment, substitution, or upgrade of any network equipment, (including, but not limited to, the addition of a VPN concentrator, a router, the introduction of a network firewall, the addition of a bandwidth device, and/or the addition of modems to the network);
 - c. Network device configuration, including but not limited to, configuration of routers, firewalls, and other network devices;
 - d. Connection or disconnection of any network devices, including servers, network printers, terminal, servers, repeaters, hubs, bridges,

switches, and routers. Any planned purchase of a network-attached device must be reviewed and approved by ITS prior to purchase.

- e. Establishment of a “*demilitarized zone*;”
- f. Negotiation and maintenance of all external network service agreements;
- g. Establishment of a Remote Access Virtual Private Network.

Because ITS has ultimate responsibility for the operation of the University’s network, ITS has the authority to make necessary changes to any part of the University’s network structure at any time. However, if changes are required, ITS will provide notification as soon as possible to non-ITS computing administrators that changes will be implemented.

A. Host Configuration and Logging Requirements

All hosts (clients and servers) connected to the University network or containing University proprietary information must comply with University standards for configuration and operation. All internal servers deployed at Saint Louis University must have a designated administrator responsible for the server’s proper configuration and operation.

In addition, all administrators of hosts containing University confidential information shall develop and implement reliable logging features to identify and track problems, threats, attacks, and suspicious activities.

At a minimum, logging shall include:

1. Security administration and changes to global security options;
2. System entry (or session initiation and termination);
3. Failed system entry and resource access attempts;
4. Read and update access to sensitive information; and
5. Update and delete access to critical information

The host administrator must monitor logged events on a regularly scheduled basis, or must ensure that an experienced and knowledgeable person monitors these events. The goal of monitoring is to identify problematic conditions or security events that include, but are not limited to:

1. Systematic break in attempts, chronologically and by account
2. Inappropriate access denials
3. Evidence of account sharing
4. Excessive access failures for a specific account or resource
5. Abnormal access patterns
6. Unusual read or update access to sensitive information

7. Deletion of critical information
8. Security changes, both administrative and system level

Any unusual or problematic event identified in the log report must be reported to the Vulnerability Oversight Committee upon discovery.

All host administrators must document the configuration of the servers or hosts, and must also describe server standards and features that will assure proper logging and tracking. ITS will provide information on proper configuration standards. The Information Security Officer will work with ITS and non-ITS staff to ensure that appropriate protection features are included in the host configuration. ITS will serve as the repository for all University host configuration descriptions.

B. User Access and Authentication Requirements

Access to Saint Louis University computing resources must be authenticated through the use of both an **account** and **password(s)**. Following are requirements for structuring accounts and account access:

Account Characteristics

1. Each account name shall be unique within the domain of the specific computing resource or *object*.
2. Accounts shall only be granted on a need-to-know basis.
3. Account privileges shall only be granted on a need-to-act basis, and are based on three main categories of account access: *basic user*, *power user*, and *system administrator*. Whenever possible, account privileges will be associated with individuals rather than groups in order to associate actions with specific users.
4. When feasible, each account should remain associated with an individual for the duration of that individual's affiliation with the University.
5. Concurrent access to an account should not be permitted.

Account Sharing

Decreased security and accountability is inherent in account sharing, therefore, account sharing is strongly discouraged and can only be used for special reasons or in limited circumstances. The supervisor of the area in which the shared account is being implemented will develop specific procedures, including methods for protecting the shared account, password(s), and data. Data Stewards (see Information Security Management policy) representing the specific data for

which shared accounts may be used, must approve the supervisors' procedures for sharing an account.

Temporary Accounts

There may be instances in which individuals who are not directly affiliated with Saint Louis University require access to University computing systems. Access to the University network may be granted through the use of a temporary account. Non-University users of such temporary accounts must agree in writing to abide by all University policies.

All temporary accounts must have a sponsor approved by the Vice President of Information Technology Services. The sponsor must be a current staff or faculty member who attests to the validity of the need for an account and accepts responsibility for the affiliation. It is the sponsor's responsibility to request and verify suspension of the account. The sponsor must also keep a log of guest users, including date/s of usage. Suspension must be requested when the justification for the account is no longer valid, or when continuation of the account would represent a risk to the University. The sponsor must also assure that the account is terminated according to the originally approved request.

Account Life Cycle

An account is created based on a justification; therefore, if the justification changes, the account or access privileges must be reevaluated.

Those responsible for permitting access through the establishment of an account, must also establish practices for the suspension or removal of an account. An account may be suspended or removed for numerous reasons, including but not limited to:

1. account activity that is suspicious or threatening to the integrity of the account, host, or IT environment
2. account inactivity,
3. change of user status
4. loss of justification of access
5. as a result of sanctions or other disciplinary action
6. for system integrity or other extenuating circumstances

C. Requirements for the Use of Non-University Equipment on University Network

In order to ensure the University's ability to provide a secure network for all its educational and business activities, the University has developed requirements for the connection of non-University equipment to the network.

In addition, ITS has developed approval processes for the connection of non-University equipment to the network based on length of connection; i.e. either “short-term” or “long-term” connection. Generally, short-term connection is defined as a connection for a single time, for limited use, and for less than a day. An example of this situation is a single class presentation using a personally owned laptop to connect to the Internet via the University’s network.

A long-term connection is defined as a connection to the University network that is needed for longer than one day, whether continual or intermittent. An example of this situation is the connection of a personally owned laptop to the University’s network on a daily basis.

In either situation, however, the following requirements apply:

1. The use of non-University owned computer equipment must adhere to the University’s Acceptable Use Policy.
2. The University reserves the right to monitor network access and appropriate use.
3. The University reserves the right to disconnect any user or equipment that causes disruption to the network environment caused by faulty equipment, software, or inappropriate use of the network.
4. The University is under no obligation to repair or maintain non-University owned hardware and bundled software.
5. The user is responsible for proof of license of any non-University owned software.
6. The University is not liable for any loss or damage to the non-University owned equipment connected to the University’s network.
7. The owner of the equipment must ensure that appropriate virus and malicious code prevention software is installed.

D. Requirements for Use of Wireless Devices

Careful evaluation of the potential use of a wireless communication network or mechanism must be conducted prior to acquisition and implementation of such equipment. This evaluation will include approval for the use of a wireless device by the appropriate Vice President or Dean and a security evaluation by the Security Review Committee. The University employee or group wishing to implement wireless technology to connect to SLU networks must provide all necessary information for this evaluation.

All access points for wireless technology are considered part of the network configuration and must comply with all University policies and standards concerning network configuration. The wireless communication mechanism(s) may not be implemented until any security concerns cited by the Security Review Committee are addressed.

Requests for wireless connectivity must contain the following documentation:

1. An explanation of the benefit(s) of the requested connection(s).
2. A description of the types of data that will be transmitted over the proposed wireless network. The Security Review Committee must reevaluate any changes or additions to these data types for security risks.
3. A complete list of all equipment, software, network devices, etc. that will be added or used.
4. A security plan for all wireless access points and connections, including access control mechanisms.
5. Complete list of users and connections utilizing the proposed wireless connection(s).
6. List of those responsible for system and security administration.

VI. Restrictions on Use of Social Security Number

These requirements are designed to reduce the risk of unauthorized disclosure of an individual's Social Security number. These requirements also apply to the use of an individual taxpayer identification number and to "derivations" based on an individual's Social Security number. Derivations might include adding a letter or digit to the SSN, changing the order of the SSN digits, adding an offset to the digits (adding an offset of 1 would make 825 become 936), or using a portion of the SSN as an identifier.

Data Stewards must review the use of Social Security numbers as identifiers in their specific areas of responsibility. Data Stewards must identify, describe, and record all practices that use this method of identification. All practices that use Social Security numbers as identifiers will be reviewed by the Information Security Committee for compliance with applicable laws and University policy.

Any proposed use of Social Security numbers as identifiers must be submitted as a request to the appropriate Data Steward prior to putting such a practice in place. The Data Steward will submit such requests to the ISC for approval. If the ISC disapproves such use, the implementation of the proposed practice will be prohibited, unless appropriate use measures outlined by the ISC are put in place.

A proposal for the use of social security numbers must include the following information:

1. Justification for using SSN or other personal identifier
2. Control mechanism for access to such information
3. Description of procedures for controlling access
4. Description of procedures for disposal of such information

VII. Requirements for Data Encryption

The encryption of electronic University information is limited to University-approved encryption algorithms in order to ensure appropriate access to University information. When encryption is used to safeguard University information, methods or tools for encryption shall meet University standards, which will be approved by the University's Information Security Committee to ensure that data is secure and that data can be retrieved. Use of encryption is permitted only when necessary, and where decryption keys and processes for access are available to authorized University personnel.

The Information Security Committee must approve encryption of University information. Generally, encryption will only be permitted under the following conditions:

-
1. The encryption key must be provided to the appropriate Data Steward and to the University Information Security Officer.
 2. ITS will provide the software for encryption and ITS (with local support staff) will configure the encryption keys, making sure that the appropriate parties can maintain access to the University-owned files.
 3. Personal files are never to be encrypted on University equipment.
 4. If University-owned information is encrypted such that only the possessor of the information has access, this may be considered theft of University property.
 5. The use of *proprietary encryption algorithms* is not allowed unless the Information Security Committee grants specific approval.

VIII. Virus and Malicious Code Prevention

All computers (clients and servers) connected to any Saint Louis University computer network must have the appropriate Saint Louis University approved software installed and routinely updated to prevent infection of computing resources by malicious code or viruses. Software and configuration for the detection and prevention of malicious code and viruses should be installed prior to the connection of any “host” (e.g. desktop/laptop, printer, network switch) to any University network. Each department, division, or operating unit is responsible for ensuring installation and maintenance of this software.

In the event that such software cannot be used on a particular operating system or platform, the Security Review Committee must be informed in order to conduct a security evaluation of the computing environment in the absence of preventative software. In addition, administrators of these systems shall apply prudent security practices to prevent infection by malicious code or viruses. When the appropriate preventative software becomes available for an operating system or platform, it must be installed on all applicable devices.

If deemed necessary to prevent infection to other networked devices or detrimental effects to the network, infected computers shall be disconnected from the network until the infection has been removed. In addition, the University has the right to limit access to University networks in the event of an emergency caused by such an infection.

ITS will provide licensed anti-virus software for University computing resources, as well as all student, faculty and staff personal computers. Any University student or employee may request this software from the ITS Customer Service Center. In addition, ITS will maintain a list of approved software for malicious code and virus prevention. Requests for evaluation of non-approved software should be submitted to the ITS Customer Service Center. The ITS Customer Service Center can be reached at 977-4000.

If ITS discovers that a particular host has been infected with malicious code or virus or is highly vulnerable to such an infection, it may take action to block that host’s access to the network in order to contain the infection and limit its impact. ITS may also block network connections to a University business associate (e.g. Tenet, SSM) if the associate’s network is infected. ITS will restore system connections when all systems are free of the malicious code or virus and configured to prevent further infections.

IX. Technology Equipment Disposal Requirements

University departments are responsible for ensuring and documenting removal of all University information from any technology device prior to its transfer outside the department, or its disposal. This requirement applies to all University-owned electronic information processing devices and media. This includes, but is not limited to, personal computers, servers, personal digital assistants, laptop computers, tablet computers,

routers, and backup tapes. The information removal process must follow the standards outlined by the University's Division of Information Technology Services, which should render all University information inaccessible.

X. Physical Security Requirements

The term "physical security" in these requirements refers to assuring a secure environment as well as controlling physical access to University-owned equipment and data. This includes the protection of building sites and equipment (and all other information and software contained within) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperature, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

Secure IT Facilities

The Division of Information Technology Services is responsible for designating certain areas as "Secure IT Facilities" for the protection of specific technology equipment and other information handling assets. A facility may be an entire building, or a portion of the building such as a room, closet, or conduit. ITS shall provide a listing of "Secure IT Facilities" to the Vice President of Facilities, and to the Director of Public Safety.

ITS shall identify an individual responsible for security of each Secure IT Facility. This individual will be responsible for the following:

1. Ensure that appropriate staff are trained and qualified to operate fire monitoring, detection, and suppression equipment.
2. Document the receipt, movement, and removal of hardware and electronic media containing confidential information to and from the Secure IT Facility.
3. Review, approve, and retain documentation of all requests for changes to the secure structure and/or IT-related contents of Secure IT Facilities.

Each Secure IT Facility shall have structural and protection attributes that meet or exceed the current standards on file with Information Technology Services. The Vulnerability Oversight Committee will review these secure facilities on a regular basis to compare the facility's attributes to the standard. Results of the review, including any variance, shall be reported to the Vice President of Information Technology Services and to the Information Security Committee.

The following access controls apply to all Secure IT Facilities:

1. An access list must be maintained that identifies who is allowed into the area, and who is allowed to “operate” equipment.
2. Visitors, contractors, and maintenance personnel shall be authenticated through appointments and identification checks, signed in, escorted, and monitored.
3. Access logs shall be archived each month and retained for a minimum of two (2) years.
4. The Information Security Committee must approve the process and responsibility for granting and revoking access.
5. The main entrance must be manned or must use cameras or card keys for access security.
6. There shall be a secure system for maintaining locks and combinations. If there is a breach involving a lock or combination, each compromised lock should be changed.
7. Access shall be monitored for violations and suspicious activities. All apparent violations shall be investigated as part of the incident response procedure.

Workstation Environment

For workstations (including laptops) in facilities other than those designated as Secure IT Facilities, Data Stewards and their designees are responsible for evaluating the environments and identifying any physical risks to the information and information handling assets.

The physical environment for workstations that access University confidential information must have limited physical access (including visual access), so that confidential information is only available to individuals with approved authorization.

Additionally, Data Stewards and/or their designees must maintain a record of the movements of hardware and electronic media, including receipt and removal, and the persons responsible for these movements.

XI. Reporting Network Abuse or Security Violations

It is the responsibility of all Saint Louis University employees, students, and affiliates to report any known or suspected network or security violation to the University’s Information Security Officer or his/her designee.

All reports are treated confidentially. Contents of reports are shared only on a need-to-know basis, with the objective of protecting both the individual making the report as well as the subject of the report. The University will take no adverse action against anyone making a report in good faith.

Individuals who wish to report an incident may do so by contacting the Saint Louis University Compliance hotline at 877-525-5669. Reports will remain anonymous.

XII. Education/Training

The Information Security Committee, in concert with the Vice President of Information Technology Services or his/her designee, shall be responsible for ensuring that all University community members are presented with the information contained in the Information Security Policy handbook. This handbook will be made available on the University's website, and education sessions will be conducted to ensure awareness and increase understanding of these policies and requirements, and to distribute additional information concerning specific ITS standards. The University's Information Security Officer will also serve as an important daily resource to the University community concerning these policies, requirements, and ITS standards.

Data stewards, as representatives of the Information Security Committee, will perform an important role by educating their respective constituencies regarding information security policies and requirements. They will also seek to ensure ISC understanding regarding users' needs.

XIII. Sanctions for Violations

Violations or suspected violations of policies or requirements set forth in the Information Security Policy Handbook shall be pursued through applicable disciplinary procedures as set forth by the affiliation of the individual (e.g. staff member, faculty member, member of a bargaining unit, student). Disciplinary action may include termination of employment, student dismissal, and/or restitution for damages.

Updated: March 5, 2007