1.3 Appropriate Use Policy

I. Introduction

Information technology ("IT"), the vast and growing array of computing and electronic data communications facilities and services, is used daily to create, access, examine, store, and distribute material in multiple media and formats. Information technology plays an integral part in the fulfillment of Saint Louis University's research, education, clinical, administrative, and other roles. Users of Saint Louis University's IT resources have a responsibility not to abuse those resources and to respect the rights of the members of the community as well as the University itself. This Saint Louis University IT Appropriate Use Policy (the "Policy" or "AUP") provides guidelines for the appropriate use of Saint Louis University's IT resources, as well as for the University's access to information about and oversight of these resources.

Most IT use parallels familiar activity in other media and formats, making existing University policies important in determining what use is appropriate. Using electronic mail ("e-mail") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. University policies that already govern freedom of expression and related matters in the context of standard written expression govern electronic expression as well. This Policy addresses circumstances that are particular to the IT arena and shall augment but not supersede other relevant University policies.

Users should familiarize themselves with any supplementary or specifically tailored policies that also govern use of information technology systems. The Division of Information Technology Services ("ITS") and other divisions that manage IT Systems may develop and promulgate system-specific policies in association with appropriate governing bodies. External service-providing organizations may also have specific usage policies. Such policies must be consistent with this Policy and provided to the Vice President/Chief Information Officer.

II. Definitions

IT Systems. These include but are not limited to the computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by Saint Louis University. For example, IT Systems include institutional and departmental information systems, faculty research systems, computers, the University's campus network, and University general access computer labs.

User. A "User" is any person, whether authorized or not, who makes any use of any IT System from any location.

Systems Authority. While Saint Louis University is the legal owner, manager or operator of all IT Systems, it may delegate oversight of a particular system to an individual of a specific subdivision, department, or office of the University ("Systems Authority" or "Systems Administrator"), or to an individual faculty member, in the case of IT Systems purchased with research or other funds for which they are personally responsible.

Specific Authorization. This means documented permission from an authorized University official.

III. Purpose

The purpose of this policy is to ensure an information technology infrastructure that promotes the basic mission and purpose of the University in teaching, learning, research, patient care, and administration. In particular, this policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and performance of IT Systems;
- To ensure that use of IT Systems is consistent with the principles and values of Saint Louis University and those principles and values that govern use of other University facilities and services;

- To ensure that IT Systems are used for their intended purposes; and
- To establish procedures for addressing Policy violations and sanctions for violators.

IV. Scope

This policy applies to all Users of IT Systems, including but not limited to University Students, faculty, and staff. It applies to the use of all IT Systems. These include systems, networks, and facilities administered by ITS, as well as those administered by individual schools, departments, University laboratories, and other University-affiliated entities.

Use of IT Systems, even when carried out on a privately-owned computer that is not managed or maintained by Saint Louis University, is governed by this policy.

This policy does not alter the University's position or policy on intellectual property ownership for faculty and research data.

V. Appropriate Use of IT Systems

Although this policy sets forth the general rules of appropriate use of IT Systems, Students, faculty, and staff should consult their respective unit policies for more detailed statements on permitted use and the extent of use that the University considers appropriate in light of the varying roles within the community. In the event of conflict between this and other specific IT policies, this Appropriate Use Policy will control.

A. **Appropriate Use.** IT Systems are established and maintained to support the research, education, clinical, administrative, and other normal functions of Saint Louis University. Personal use of IT Systems that is not compatible with the University mission and subject to the provisions of this policy as provided in Section V.C., is also allowed; however, the particular purposes of any IT System, as

well as the nature and scope of personal use may vary according to the duties and responsibilities of the User or the type of personal use.

B. **Proper Authorization.** Users are entitled to access, modify, or delete only those elements of IT Systems that are consistent with their authorization. Any attempt to accumulate unauthorized information or misuse of information appropriately obtained is strictly prohibited.

C. **Specific Proscriptions on Use.** The following categories of use are inappropriate and prohibited:

1. **Use that impedes, interferes with, impairs, or otherwise causes harm to the authorized activities and responsibilities of others.** Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including, without limitation, "resource hogging," misuse of mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading e-mail or postings widely and without good purpose), or "bombing" (flooding an individual, group or system with numerous or large e-mail messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2. **Use that is inconsistent with Saint Louis University's non-profit status.** The University is a non-profit, tax-exempt organization, and as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-Saint Louis University purposes is generally prohibited, unless specifically authorized and permitted under other University policies. Prohibited commercial use does not include communications and exchange of data that furthers the University's educational, administrative, research, clinical, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.

   Use of IT Systems in a way that suggests University endorsement of any political candidate or political initiative is also prohibited. Users must refrain

from using IT Systems for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation with an authorized University official.

3. **Use in violation of University Policy.** Use in violation of other University policies or use that is inconsistent with the University's Catholic Jesuit mission and ideals also violates this policy. Such other University policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, conduct codes of the various schools and colleges, and specific University departmental and work-unit policies and guidelines regarding incidental personal use of IT Systems.
4. **Use damaging the integrity of the University or other IT Systems.** This category includes, but is not limited to, the following six activities:
    a. **Attempts to defeat system security.** Users must not defeat or attempt to defeat any IT System's security - for example, by "cracking" or guessing and applying, possessing, and/or using the identification or password of another User, or compromising room locks or alarm systems. (This provision does not prohibit ITS or Systems Administrators from using security scan or other similar programs within the scope of their Systems Authority.)
    b. **Unauthorized access or use.** The University recognizes the importance of preserving the privacy of Users and data stored in IT systems. Accordingly, Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non-Saint Louis University organization or individual may not use non-public IT Systems without specific authorization.

        Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-Saint Louis University organizations or individuals across the Saint Louis University network without specific authorization. Similarly, Users are

prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System.

Users must not intercept or attempt to intercept or access data communications not intended for that User, such as promiscuous network monitoring, running network sniffers, or otherwise tapping phone or network lines.

ITS staff is prohibited from engaging in any intrusive investigations not authorized in accordance with ITS Policy on intrusive investigations.

c. **Disguised use.** For purposes of this policy, Users are prohibited from masquerading as, or impersonating others.

d. **Distributing computer viruses.** Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

e. **Unauthorized equipment modification.** On shared-use IT Systems that serve departmental or University enterprise-wide functions, Users may only perform additions, removals, or modifications to the equipment with the approval of the appropriate Systems Authority.

f. **Use of unauthorized devices.** Without specific authorization, Users may not physically or electronically attach any network device (such as a server) to IT Systems. Upon request, a User shall promptly remove any unauthorized network device.

5. **Use in violation of law.** Any use of IT Systems in violation of civil or criminal law at the federal, state, or local levels is prohibited. Examples of such use includes, but is not limited to:

    - promoting a pyramid scheme;
    - distributing illegal obscenity;
    - receiving, transmitting, or possessing child pornography;

- infringing copyrights; and
- making bomb or other threats.

With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

6. **Use in violation of University contracts or licenses.** All use of IT Systems must be consistent with the University's contractual obligations, including limitations defined in software and other licensing agreements.
7. **Use in violation of external data network policies.** Users must observe all applicable policies of external data networks when using such networks.
8. **Free Inquiry and Expression.** Users of IT Systems may exercise rights of free inquiry and expression consistent with provisions contained in the Student Handbook, the Faculty Manual, or the Staff Handbook, as may be appropriate, and the principles of academic freedom at Saint Louis University.
9. **Personal Account Responsibility.** Users must maintain the security of their own IT Systems accounts and passwords, and they are responsible for any breaches in the security of those accounts or passwords which are caused by their own negligence, recklessness or unlawful actions. Any User changes of password must follow prescribed guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users have the responsibility to control the activities which they permit others to carry out under their IT System accounts or passwords or on their personal web pages.
10. **Encryption of Data.** University faculty and staff are authorized to encrypt files, documents, and messages for protection against unauthorized disclosure while in

storage or in transit. Any encryption of University-related data performed on an IT System must use software and protocols endorsed by ITS and such encryption must permit properly designated University officials, upon the direction of the Vice President/Chief Information Officer, to decrypt the information. Upon request of the Vice President/Chief Information Officer, a User shall decrypt any encrypted information, including without limitation, data, documents and messages.

11. **Responsibility for Content.** Official University information may be published in a variety of electronic forms. The individual under whose auspices the information is published is responsible for the content of the published document.

    Users may publish information on IT Systems or over Saint Louis University's networks. Neither Saint Louis University nor individual Systems Administrators can screen such privately published material, nor can they ensure its accuracy or assume any responsibility for its content. The University will treat any electronic publication provided on or over IT Systems that lacks the authorized authority of an appropriate University official as the private speech of an individual User.

12. **Registration of equipment.** Upon notice to the User, the Division of Information Technology Services may require Users to register any equipment or devices utilizing IT Systems, whether or not such equipment is personally owned or located on the property of the University.

13. **Personal Identification.** Upon request by a Systems Administrator or other University authority, Users must produce valid University identification.

14. **Privileged Access.** Users with higher levels of privileged access to IT Systems, for example Systems Administrators, Application Security Administrators, and Database Administrators, may be subject to additional constraints on the use of that privileged access as described in policies and procedures for intrusive investigations, administrative application account administration, confidentiality agreements, and other similar documents.

VI. University Access Without Consent of User

The University places a value on privacy and recognizes its importance in an academic setting. There are circumstances nonetheless in which, following prescribed processes and procedural safeguards established to ensure access is gained only when and to the extent appropriate, the University may determine that certain University concerns outweigh the value of a User's privacy and warrant University access to relevant IT Systems without the consent or knowledge of the User. Accordingly, in the circumstances described below, use of University IT Systems should not be considered to be private.

A. **Conditions for Access.** In accordance with state and federal law and published University policies, the University may access any aspects of IT Systems, without the consent or knowledge of the User, in the following circumstances:

   1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems;
   2. When required by federal, state or local law;
   3. When there are reasonable grounds to believe that a violation of law or a breach of any of the proscriptions of Section V.C., of this Appropriate Use Policy may have taken place and access and inspection or monitoring may produce evidence related to the suspected misconduct;
   4. When such access to IT Systems is required to carry out essential business functions of the University; or
   5. When required to preserve public or campus health, safety, or order.

B. **Process.** Consistent with the privacy interests of Users, University access without the consent or knowledge of the User will occur only with the approval of the President, Provost, or their designee or the Vice President/Chief Information Officer, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public or campus health, safety, or order or when such access is necessary for IT Systems maintenance when such is conducted in accordance with established procedures and in accordance with provisions of Section VI.A.

C. **User access deactivations.** In addition to accessing the IT Systems, the University, through the appropriate Systems Administrator, may deactivate a User's access privileges, when the User is suspected of any violation of this or other Policy or when such action is necessary for investigation. The Systems Administrator will attempt to notify the User of any such action if appropriate.

D. **Use of security scanning systems.** By attaching (either physically or virtually) privately owned personal computers or other IT resources to the University's network or other IT Systems, Users consent to University use of scanning programs or other security mechanisms on those resources while they are attached to the network when the use of such scanning systems is necessary and is consistent with the other provisions of this Policy.

E. **Encrypted material.** Encrypted files, documents, and messages may be accessed by the University under the guidelines set forth in Sections VI.A, and VI.B, above.

VII. Security

Users of IT Systems should be aware that IT Systems and the information contained therein are not necessarily secure.

VIII. Enforcement Procedures

A. **Complaints of Alleged Violations.** An individual who believes that they have been harmed by an alleged violation of this policy may file a complaint in accordance with established University Grievance Procedures (including, where relevant, those procedures for filing complaints of sexual harassment or any form of harassment) for Students, faculty, and staff. The individual is also encouraged to report the alleged violation to the Systems Authority overseeing the facility most directly involved, or to the Vice President/Chief Information Officer, who shall investigate the allegation and (if appropriate) refer the matter to an appropriate University official, University disciplinary committee, Office of Human Resources, Department of Public Safety, and/or appropriate law enforcement authorities.

B. **Reporting Observed Violations.** If an individual has observed or otherwise is aware of a violation of this policy, even though the individual has not been harmed by the alleged violation, they are encouraged to report such evidence to the Systems Authority overseeing the facility most directly involved, or to the Office of the Vice President/Chief Information Officer of the University.

C. **Disciplinary Procedures.** Alleged violations of this Policy will be pursued in accordance with the applicable disciplinary procedures for Students, faculty, and staff, as outlined in the Student Handbook, Faculty Manual, Staff Handbook, various other policy manuals and applicable materials or if appropriate, through criminal or civil court proceedings. Staff members who are members of University-recognized bargaining units will be disciplined for violations of this policy in accordance with the relevant disciplinary provisions set forth in the agreements covering their bargaining units.

   Systems Administrators and employees of ITS may be required to participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, Systems Administrators or the Vice President/Chief Information Officer, or their designees are authorized to investigate alleged violations.

D. **Temporary Suspension.** The Vice President/Chief Information Officer of the University, or their designee, is authorized

   - to invoke a temporary suspension from use of, or access to, any or all IT Systems whenever in their sole judgment such action is necessary to comply with any federal, state or local law, ordinance, rule, or order;
   - to preserve the security or integrity of the IT Systems and/or University facilities;
   - to protect a User's physical or emotional safety or well-being; or
   - to preserve public or campus health, safety, or order.

E. **Penalties.** Individuals found to have violated this policy may be subject to penalties provided in other University policies dealing with the underlying

conduct. Violators may also incur other IT-specific penalties, including, without limitation, temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the applicable Systems Administrator or the Vice President/Chief Information Officer, if desired.

F. **Legal Liability for Unlawful or Inappropriate Use.** In addition to University discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful or inappropriate use of any IT System.

G. **Appeals.** Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

IX. Policy Development

This policy may be periodically reviewed and modified. Requests for review or modification to this Policy may be submitted to the Vice President/Chief Information Officer. Modifications may be developed by the Vice President/Chief Information Officer in consultation with appropriate University committees, Students, faculty, and staff. Any material change to this policy must be approved by the President of the University.

Questions relative to this policy should be directed to the Vice President/Chief Information Officer.