Motivated by convenience, speed and cost-effectiveness, electronic mail (e-mail) increasingly has become a primary means of communication at Saint Louis University (SLU). As a result, many official University announcements, including emergency and safety notifications, now are communicated to students, faculty and staff in this manner.

Automating the distribution of e-mail to all members of a group or particular mailing list has become a critical component of scholarly collaboration. To help automate this process, the University has opted to utilize a feature commonly referred to as a Listserv, best defined as an electronic mailing list that simultaneously disseminates information to large numbers of e-mail addresses. In addition, many colleges and universities across the country have employed them to facilitate and enhance classroom education as well as for the day-to-day administration of the organization.

The purpose of this policy is to ensure the appropriate use of the University’s Listserv capabilities, as defined in part by both the Saint Louis University Electronic Mail Policy and Saint Louis University Information Technology Appropriate Use Policy. Furthermore, the policy is designed to help ensure that:

- Listservs are used ethically, in compliance with all applicable laws/regulations and policies, including policies established by the University and its operating units;
- Data Stewards and Listserv Managers are informed of how concepts of privacy and security apply to mailing lists; and
- Disruptions to University e-mail and other services and activities are minimized.

The University recognizes that academic freedom, freedom of speech, privacy, and confidentiality are all important principles which must be protected. Therefore, each principle is addressed within the context of the limitations imposed by the University’s legal and policy obligations.
2. All University Listserv records, Listserv names and contents, whether manually or automatically generated;
3. All users of University Listserv application accounts; and
4. All users of Listserv functions provided by the University, regardless whether generated on University or non-University computers.

This policy does **not** apply to:
1. Distribution groups provided by the University e-mail system;
2. Printed copies of Listserv material. However, other laws and/or policies may apply to such documents; and
3. Listserv Managers or Authorized Senders using Listserv functions to mass mail users of non-University e-mail accounts for approved University business.

### 4.0 DEFINITIONS

**4.1 Ad Hoc Listserv** - A Listserv created by ITS upon request. The recipient list is managed by Listserv Managers.

**4.2 Authorized Sender** – A user approved by the Ad Hoc Listserv Manager or Data Steward to send messages to a Listserv.

**4.3 Automated Listserv** – A Listserv created by ITS in which the recipient list is automatically updated based upon changes in University information systems made by the Office of the Registrar, Human Resources (personnel, departmental, organization or group) or individual academic/administrative units.

**4.4 Confidential Information** – For individuals, confidential information is a combination of any information that identifies and describes an individual, including his or her name in conjunction with social security number, protected health information and financial account information. From a business perspective, confidential information refers to any type of information that may have a negative impact if shared with others who do not need to know, including attorney/client information, University financial information, research information and business proposals and contracts.

**4.5 Data Steward** – Individuals ultimately responsible for the definition, management, control, integrity, or maintenance of a departmental or enterprise data resource.

**4.6 Listserv** – An electronic mailing feature that can send simultaneous messages to multiple e-mail addresses on a mailing list.

**4.7 Ad Hoc Listserv Manager** – Person(s) who administer Ad Hoc Listservs by managing the recipient list and approving Authorized Senders within the Listserv application.

**4.8 Protected Health Information (PHI)** – Individually identifiable health information transmitted or maintained in any form.

**4.9 Information Resources** – Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving e-mail, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to,
mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

4.10 Information Security Officer – The designated person who monitors overall compliance with University information security policies and procedures, making recommendations for improved security and for monitoring the occurrence of security incidents. The Information Security Officer serves as the HIPAA Security Officer.

4.11 Organizational Unit – An entity within the University that operates as a distinct function, such as a department, division, business unit, school, college and/or library.

5.0 POLICY

Ad Hoc Listservs: Authorization and Provision

5.1. Ad Hoc Listservs will be provisioned upon request and may require approval from the respective Data Steward(s). The following Ad Hoc Listservs always require approval and should be directed appropriately:

5.1.1. Saint Louis Campus student organizations must obtain approval from the Assistant Vice President and Dean of Students, or designee.

5.1.2. Madrid Campus student organizations must obtain approval from the Director of Student Life, or designee.

5.1.3. Madrid Campus non-student groups or organizations must obtain approval from the Vice President and Rector for Madrid, or designee.

5.2. Organizational units may develop supplemental policies that specify additional requirements, structure or restrictions on who may request Ad Hoc ListServs or who may serve as an Ad Hoc Listserv Manager.

5.3. A department chair, or designee, shall serve as the Ad Hoc Listserv Manager for any SLUCare clinic Listservs.

5.4. A faculty or staff advisor shall serve as the Ad Hoc Listserv Manager for the respective student organization.

5.4. Ad Hoc Listserv Managers are given logical access to the Listserv application and must:

5.4.1. Maintain the Listserv recipient list;

5.4.2. Ensure the confidentiality of e-mail addresses included in the Listserv;

5.4.3. Approve and manage the Authorized Senders;

5.4.4. Manage the appropriateness of content distributed;

5.4.5. Manage the appropriate use of the Listserv in compliance with the Saint Louis University Information Technology Appropriate Use Policy; and
5.4.6. Protect the security of access to the Listserv application in compliance with Section V.E of the Saint Louis University Information Technology Appropriate Use Policy.

**Automated Listservs: Authorization and Provision**

5.5. Data Stewards for Automated Listservs must:

5.5.1. Set the criteria which allows for automatic maintenance of the Listserv recipient list; and

5.5.2. Approve and manage the Authorized Senders to the respective Listserv.

5.6. The Registrar, or designee, acts as the Data Steward for Automated Listservs pertaining to student course lists.

5.7. The Vice President of Human Resources, or designee, acts as the Data Steward for Automated Listservs pertaining to faculty and staff lists.

**Use of Listservs**

5.8. Authorized Senders must utilize Listservs appropriately and in compliance with Section V of the Saint Louis University Information Technology Appropriate Use Policy.

5.9. Listservs found to be outside the original stated purpose of the Listserv or in violation of the Saint Louis University Information Technology Appropriate Use Policy may be denied or removed at the discretion of the Data Steward or the Vice President and Chief Information Officer, or their designees.

5.10. Authorization to distribute messages to University-wide Listservs requires approval by the Associate Vice President for Marketing and Communication or the Vice President and Chief Information Officer, or their designees.

5.11. Listserv messages may not exceed 1MB in size.

**Removal of Listservs**

5.12. Ad Hoc Listservs which have been inactive for a period of 180 days or more will be removed. Listserv Managers will be notified via e-mail two weeks prior to account removal. It is the responsibility of the Listserv Manager to obtain any pertinent data from the Listserv prior to the removal date.

5.13. Automated Listservs that have been inactive for more than 365 days will be identified through an annual audit. ITS will seek approval of the Data Steward prior to removing the Listserv.

**University Property**

5.14. Listservs are the property of the University. All material distributed using Listservs are subject to University policies and applicable law.

5.15. Any Listservs assigned by the University to individuals, sub-units, or functions of the University remain the property of the University. Access to Listservs or e-mail addresses contained within the Listserv may not be loaned or sold.
Confidentiality

5.16. Authorized Senders and Listserv Managers must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed and stored by others. Users must exercise discretion and obtain appropriate organizational unit approvals when using a Listserv to communicate confidential information.

5.17. A user's request to be removed from Ad Hoc Listserv(s) will be accommodated when possible and as appropriate. Exceptions include Listservs managed by Human Resources, the Registrar, and/or Marketing and Communications used to communicate to University e-mail accounts.

Service

5.18. Users with requests, questions, or issues relating to Listservs may contact:

5.18.1. Saint Louis Campus IT Service Desk at 977-4000
5.18.2. Madrid Campus IT support at 91-554-58-58 ext. 262 or 263, or at support@madrid.slu.edu

6.0 DOCUMENT CONTROL

At a minimum, this policy will be reviewed and approved annually. While changes to this policy and associated procedures may be necessary from time to time, all changes to this policy will be reviewed and approved as described in the Policy Approvals section of this policy. All policy and associated procedure documentation, including a record of all changes, will be maintained by the ITS Quality Assurance Office and is available for inspection.

7.0 RESPONSIBILITIES

The President of the University is responsible for the general and active management, control and direction of the business operations, educational activities and other affairs of the University, and also the development and implementation of all of the University’s policies.

It is the responsibility of all Listserv Users to read, understand, and follow this policy. Authorized Senders, Ad Hoc Listserv Managers, and Data Stewards have additional responsibilities as outlined above.

8.0 OVERSIGHT

The Information Security Officer is the ITS Director of Quality Assurance and is responsible for monitoring overall ITS compliance with confidential information security policies and procedures, making recommendations for improved security and for monitoring the occurrence of security incidents.

9.0 INTERIM POLICIES

The President of the University and the Vice Presidents may establish and implement an interim policy in situations where this University policy must be amended in a time period too short to permit the completion of the process delineated in this policy. An interim policy may remain in force for up to six months from the date of issuance.
10.0 POSTING OF POLICIES

All University policies will be posted on the official University website. The Vice Presidents, or their designees, will identify all of the places in University communications where a policy appears and ensure standardization of print and on-line policies. All organizational unit web pages must link to the official University policy website instead of posting their own versions of the approved policy. The Vice Presidents shall review and approve printed versions of University policies that are referenced in the Faculty Manual, Staff Handbook, Student Handbook, or other communications prior to their publication. All printed versions of University policies must include a disclaimer that the official University policy website should be consulted for the latest version.

11.0 RELATED PROCEDURES AND GUIDELINES

Organizational units may develop supplemental academic or administrative policies that pertain to their units. These specific policies may augment, but not conflict, with this policy. It is the responsibility of the Dean or comparable administrator to seek the pertinent Vice-Presidents’ approval before implementing such policies. It is likewise the responsibility of the Dean or comparable administrator to review such policies for consistency with University policies.

Associated policies and procedures include:

1. Saint Louis University Information Technology Appropriate Use Policy
2. Saint Louis University Electronic Mail Policy

12.0 POLICY VIOLATION

Alleged violations of this Policy will be pursued in accordance with the applicable disciplinary procedures for faculty, staff, and students, as outlined in the Faculty Manual, Staff Handbook, Student 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.

13.0 POLICY APPROVALS

The Vice Presidents will solicit, as appropriate, the advice of the Council of Academic Deans and Directors, Faculty Senate Executive Committee, Staff Advisory Committee, Student Government Association, and Office of General Counsel before University policies are sent to the President’s Coordinating Council for review and approval.

Some policies also may require the approval of the Board of Trustees if it is so stipulated in the University By-Laws or if other established policy or legitimate past practice suggests that Board approval would be desirable.