SAINT JOSEPH’S UNIVERSITY
INFORMATION SECURITY POLICY

1. STATEMENT
   POLICY STATEMENT

Saint Joseph’s University (“the University”) is committed to safeguarding the Confidentiality, Availability and Integrity of its Information Resources. The University adopts and implements this Information Security Policy (“Policy”) to reduce the risk of a Security Incident.

1.2 POLICY SCOPE

   Persons
   This Policy applies to anyone who accesses the University’s Information Resources, including students, faculty, staff, alumni, contractors, consultants, third parties, guests and volunteers of the University.

   Information Resources
   This Policy applies to all Information Resources, including those under contract or license of the University, recorded on any type of media, stored by or within any University software application, stored in a database or file folder on any University computer or storage system, accessed through the University’s telecommunications and networking equipment, transmitted through the University’s email system, or posted on the University’s external or internal web sites.

   Classification of Information
   This Policy applies to Confidential, Internal Use and Unrestricted Information.

2 PHILOSOPHY

As defined in Plan 2010: The Path to Preeminence, the University’s mission is to strive for academic excellence in all programs, emphasize its Catholic intellectual tradition, improve diversity in enrollment, staffing and course offerings, provide improved access to Jesuit education and promote justice and service to others. Toward these ends, the University provides access to computing and information resources for students, faculty, staff and other constituents, within institutional priorities and financial capabilities.

Annually, all users of the University’s information resources are required to read, agree to and electronically sign the “User Responsibility Statement” which is presented to all users through the University’s information portal each year. Users must ACCEPT the terms of the statement in order to access the University’s information resources. This process allows the University to capture virtually everyone’s acceptance of the policy annually and it is tracked through the University’s ERP systems.

3 RESPONSIBILITIES

All members of the University community are responsible for protecting the Information Resources for which they have access. Six roles – User, Unit Head, Data Steward, Information Security Personnel, Information Security Officer and Information Technology Service Provider – are identified and defined below, with their respective responsibilities. Members of the user community can be assigned to multiple roles and, as such, have different levels of responsibilities for each of role.
3.1 Users

Users include the students, faculty, alumni, contractors, consultants, third parties, guests and volunteers of the University, regardless of whether they actually access Information Resources. They are responsible to work within the guidelines of this Information Security Policy and other supporting security related policies referenced within and must understand and comply with current policies, guidelines, procedures and protocols. Users are responsible for protecting Information Resources to which they have access. It is essential that Users not share or compromise passwords. Further, Users must not store passwords on personal computers in an unencrypted fashion or display their password on paper notes near their computer. Users are responsible for securing their Electronic Resources against unauthorized access when left unattended. Users are responsible for the physical security of their computers and Electronic Resources in their office and on-campus living areas. Doors must be locked to protect these resources when an area will be unattended for any period of time. Users with portable devices such as PDAs and laptop computers must be especially careful and attentive in protecting and securing these devices. It is the responsibility of the User to report any policy violations to the Unit Head or Data Steward for the specific information resource or the University’s Information Security Officers.

3.2 Data Steward

The Data Steward has all the responsibilities defined in the User role. Additionally, Data Stewards are responsible for the overall accuracy, integrity and consistency of data within their respective area of responsibility. They must create and maintain a secure office environment with regard to electronic data. Data Stewards must establish and enforce sound policies and procedures to manage the Information Resources assigned to them. Data Stewards are responsible for reviewing and authorizing requests for access to the data in their purview. Access to data is granted to requesters who require the information to perform their job-related duties. Data Stewards are responsible for training users who have been granted data access to ensure proper understanding and Acceptable Use of the data. Data Stewards must immediately report all security violations to the Information Security Officers to ensure the violation is contained and addressed appropriately.

See the University’s Data Stewardship Policy at http://www.sju.edu/int/resources/it/policies/datastewardship.html.

3.3 Unit Head

The Unit Head has all the responsibilities defined in the User role and, in most cases, has stewardship responsibilities for data that originates within the Unit. Additionally, the Unit Head is charged with the administration of this Policy within the Unit. The Unit Head must comply with the current policies, guidelines, procedures and protocols, leading by example those who work within their unit. The Unit Head must create and maintain a secure office environment with regard to electronic data. The Unit Head is responsible for authorizing and terminating access to Information Resources for staff within the Unit. When necessary, the Unit Head will coordinate with Data Stewards to acquire the necessary access for staff within their Unit. The Unit Head must ensure that staff is properly trained before using any Information Resource. It is the responsibility of the Unit Head to address any policy violations reported to them by their direct reports. Unit Heads must immediately report all security violations to their immediate supervisor, appropriate Data Steward or Information Security Officers to ensure the violation is contained and addressed appropriately.
3.4 INFORMATION SECURITY PERSONNEL

Information Security Personnel are responsible for specific areas of the University’s network and information resources. The incumbents of these positions are responsible to perform their duties in accordance with the current security policies, guidelines, procedures and protocols and upon discovery, immediately report security breaches and vulnerabilities to their manager and the Information Security Officers. Information Security Personnel have all the responsibilities of the User and Data Steward roles along with the specific responsibilities that come with being in an Information Security position.

Director of Database Administration – The Director of Database Administration is responsible for the availability, integrity, security and performance of the University’s databases including the ERP, Portal and Learning Management Systems, as well as web application servers used to access these databases.

Systems Administrator – The Systems Administrators are responsible for the availability, integrity, security and performance of network servers, storage devices, tape and backup systems in the University’s network infrastructure.

Portal Administrator – The Portal Administrators are responsible for the availability, integrity, security and performance of the University’s information portal, learning management system and identity management systems.

Director of Network Services – The Director of Network Services is responsible for the availability, integrity, security and performance of the campus network including network electronics, management software, and all devices that comprise the network infrastructure.

Director of Telecommunications – The Director of Telecommunications is responsible for the availability, security and performance of the campus telecommunication systems including PBX, cabling plant, and the technology that connects the University to the telecommunications service providers.

3.5 INFORMATION SECURITY OFFICERS

The Information Security Officers are the members of the Information Technology Executive Management team which includes the Assistant Vice Presidents for Information Technology, the Executive Director of Web and Support Services and the Executive Director of Instructional Technology and Distributed Learning. The Information Security Officers work collaboratively with the Information Technology Advisory Council (ITAC) and the ITAC Information Security Sub Committee on Information Security matters. The Information Security Officers have overall responsibility to implement the University’s Information Security policy. The Information Security Officers are responsible for the security of the University’s network and information resources including the technology, telecommunications services, data creation, storage, physical transport, electronic transmission and the security monitoring of all of the above mentioned areas. The Information Security Officers are further responsible to lead the University in all information security procedures and protocols, providing policies and procedures, selecting and implementing new security controls as necessary, and providing periodic security updates to the University community.

3.6 INFORMATION SERVICE PROVIDERS

Information Service Providers include divisions, departments or individuals who manage significant information resources and systems and make these resources available to others. Information
SAINT JOSEPH’S UNIVERSITY
INFORMATION SECURITY POLICY

Service Providers include Information Technology, the Drexel Library, Provost’s Office, Enrollment Management, the College of Arts and Sciences, the Haub School of Business, the College of Professional and Liberal Studies, the Office of Planning, the Facilities Management and Public Safety offices, the Early Responders and Distance Learning Center, the Financial Affairs division and other entities that operate at school, division or department level.

Information Service Providers are responsible for managing access to and ensuring the security of the systems that they support. They are responsible for developing and enforcing policies and procedures with respect to these resources. Additionally, the providers are responsible for developing and maintaining business continuity plans to address significant service interruptions.

The Providers are responsible for physically protecting the servers, client computers, network equipment, cabling and other electronic devices under their purview. Power, temperature, alarms and fire monitoring devices should be deployed as needed. Providers must ensure that the location where equipment is housed is physically secure and that alarms and surveillance cameras are installed as required.

The Providers must implement authentication and authorization technologies that are utilized and supported on the University network. Providers must ensure that software including operating systems is maintained and updated with relevant software patches and updates.

4 ACCEPTABLE USE

All Users of the University’s network and information resources must abide by the “Guidelines for the Use of Computing and Network Resources” policy in order to continue usage and avoid disciplinary action, which could include monetary fines, expulsion (students) or termination (employees).

To review the entire policy, refer to:

http://www.sju.edu/int/resources/it/policies/usage.html

5 PROTECTION OF UNIVERSITY INFORMATION RESOURCES

5.1 BARBELIN DATA CENTER AND OTHER COMPUTER FACILITIES

Physical access (i.e. swipe and key) to the Barbelin Data Center and other computer facilities that comprise the University’s technology infrastructure is limited to Information Technology (IT) personnel whose position responsibilities require access to those areas.

Access to computer facilities must be authorized by the IT Executive Management team (i.e. Assistant Vice Presidents and Executive Directors). Key and/or ID swipe card access is granted to employees in the following IT positions:

Information Technology AVPs and Executive Directors
Systems Administrators
Network Administrators
Database Administrators
Operations
IT Support Technicians

The Data Center Access Policy defines in greater detail the guidelines for authorizing access to the Barbelin Data Center.

6 PRIVACY
The University collects and retains information and data about its students, employees, alumni and friends in support of the teaching, learning, research and service mission of the University. The University is committed to protecting and maintaining the privacy of this information. Access to University information is restricted to faculty, administrators and staff who need that information in order to perform the duties of their position. Employees with access to this information may use it only for the purposes of fulfilling the duties and responsibilities of their positions and in accordance with applicable privacy laws.

With regard to its students, the University has prepared a policy for protection of highly sensitive information and it is entitled, “Policy on Confidentiality of Student Records”. The policy may be reviewed at:

http://www.sju.edu/int/resources/registrar/csrpolicies.html

For related information, see the University’s Data Stewardship and Banner Data Stewardship policies.

7 IDENTITY MANAGEMENT AND ACCESS CONTROL
The University has developed automated processes for identity management purposes. These processes manage the addition, modification and deletion of network accounts and the roles and privileges assigned to account holders. In order to access any resource on the University network, faculty, staff, students, alumni and guest must first have their demographic and biographic information entered into the University’s Banner system. Once an acceptable profile has been established within the system, a network account will be created for the User and the User will be assigned one or more roles (e.g. student, employee) based on the profile. Users are assigned the appropriate set of privileges based on their role(s) at the University.

A University administrator must sponsor and approve any person who is requesting guest account privileges. Guest accounts are created after the guest’s demographic and biographic information is entered into the University’s ERP system. All guest accounts are created with an expiration date and these accounts become deactivated once the expiration date has passed.

Use of shared or generic accounts should be avoided whenever possible.

For additional details on Identity Management and Access Control, refer to the Account Administration Policies and Procedure document.

8 CLASSIFICATION OF DATA
University data is classified into levels of sensitivity and risk. It is the responsibility of all Users especially Data Stewards, Unit Heads and Information Security Personnel to protect the
confidentiality of University data based on the classification level assigned to the data. The levels of classification are as follows:

Confidential - Confidential data is sensitive, high-risk information about an individual or the University. Confidential data includes data that the University is required to protect under legal or regulatory provisions. For example, confidential data includes information protected by the Family Educational Rights and Privacy Act (FERPA) such as student academic history, judicial records and financial records. Other confidential information includes social security numbers, employment and benefit information, health information, alumni giving, research information, privileged communications and other sensitive data. Confidential information also includes Covered Accounts which are student accounts or loans that are administered by the University.

Internal Use - Internal Use data is information that requires some degree of protection and is specific to University operations including internal memos, policies and correspondence.

Unrestricted - Unrestricted data is information that is generally available and open to the public including information found on the University external web sites such as faculty and staff names, titles, department information, work phones, class schedules and other such information.

When a User is unsure of the classification status of data, the User should assume that the data is classified for Internal Use and should protect the data as appropriate.

9 PASSWORD MANAGEMENT

Users are responsible for all actions performed using their account and for protecting their passwords. Under no circumstances should a password be shared with anyone. If users suspect that their password has been compromised, they must reset their password using the “Forget Password?” link on the MySJU login page at http://my.sju.edu.

All users are required to change their passwords periodically. Most faculty, staff and students are required to change their password annually while users of the University’s Banner ERP system must change their passwords every six months. When changing their password, users are required to establish a new password with a minimum length of six characters and with at least one number and one alphabetic character. When changing passwords, users are not permitted to select passwords that have been used in the past two years.

To password management policy may be reviewed at: http://www.sju.edu/int/resources/it/policies/password.html

10 RISK MANAGEMENT

On an annual basis, a risk assessment is conducted by external auditors to review access policies, procedures and controls. The audit ensures that only authorized users can gain access to the University’s network and systems. In addition, the audit will review IT operations, general security, application controls, and database, network and system administration.
### 11 CONTINGENCY PLANNING

The Office of Information Technology has a Disaster Recovery Plan for the Data Center and for the Banner ERP system. In the event of the loss of the Barbelin Data Center, the Office of Information Technology would relocate its data center to its off-campus, DR site and endeavor to restore core technology services (e.g. Banner ERP) within 24-48 hours, and portal and course management systems within 3-5 business days.

The disaster recovery of the Banner platform is tested on an annual basis with involvement from the user community. The outcomes of the DR test are documented and the Banner DR plan is updated accordingly.

The IT recovery documents for the Data Center and Banner are confidential and not published for the University community or public. For more information about these DR plans, please contact the IT Executive Management Team.

Service Providers are responsible for all aspects of contingency planning for their respective system. It is the responsibility of the Service Provider to document the disaster recovery plans for his/her system and to conduct periodic DR tests of the systems.

### 12 INCIDENT MANAGEMENT

All information technology incidents will be reported and documented using the IT work order system. Incidents will be triaged by the IT Help Desk staff and assigned to the appropriate work queue for problem resolution. The IT Executive Management Team will manage their respective work queue and ensure that all incidents are addressed and resolved in a timely manner.

### 13 SECURITY COMPLIANCE AND MONITORING

Access to critical network resources, applications and databases are monitored and reviewed by the systems, network, portal administration and data base administration teams. Logs are reviewed weekly, and in some cases, daily by administrators to ensure that key systems are secure and inappropriate access requests are identified, logged and investigated. Monitoring activities are logged using the IT work order system. The Information Security Officers are notified of any security violations, breaches or anomalies that are found.

### 14 CHANGE MANAGEMENT

Systems, network, database and application changes are tracked using the IT work order system. Systems, network and database changes are authorized and approved by the Information Security Officers or their designee. Application changes are tested and approved by the security officer for the requesting area.

### 15 DATA BACKUPS AND OFFSITE STORAGE

Key production servers are incrementally backed up on a daily basis. A full backup is performed on these servers weekly.

A full backup of the Banner production database is performed daily and stored at the on-campus DR site. Banner database log files are captured every 15 minutes and copied to the on-campus...
SAINT JOSEPH’S UNIVERSITY
INFORMATION SECURITY POLICY

DR site. Incremental backups of the Blackboard and Luminis databases are done daily and a full backup is performed weekly.

On a weekly basis, tape backup of all Banner/Oracle production systems is completed and the tapes are stored off-site. The off-site tapes are kept in an off-campus storage vault for one month.

Data synchronization of first tier production systems (i.e. Banner, Blackboard, University web site) is maintained with storage devices housed at the University’s off-campus DR site.

16 ENFORCEMENT

There are penalties for abuse of Information Resource privileges in violation of this Policy. Every user is expected to uphold the integrity, availability and confidentiality of the University’s information resources.

Failure to comply with this policy is subject to disciplinary action. If sufficient information that misuse of the information resources has occurred, any or all of the following steps will be pursued to protect the user community.

- Notify the User’s project director, instructor, academic advisor or administrator officer of the investigation.
- Refer the matter for processing through the University’s discipline systems.
- Suspend or restrict the user’s access to Information Resources during the investigation. Disciplinary action may include the loss of computing privileges and other disciplinary actions up to and including non-reappointment, discharge, dismissal, and legal action, including in some cases civil or criminal prosecution under Title 18 C.A., § 5742 (1990), or other appropriate legislation.

17 RESOURCES

Information resources supporting this Policy are available on the SJU website at http://www.sju.edu/int/resources/it/policies/infofor/index.html.

18 APPROVAL HISTORY

Approved by Cabinet: September 29, 2009

19 REVIEW CYCLE

This Policy will be reviewed and updated on an annual basis. More frequent updates will occur as required by changes in the University’s computing and information resources based on the recommendations of the Assistant Vice Presidents of Information Technology, the Risk Management Committee or Information Security Sub-Committee of the Information Technology Advisory Council.
Glossary

1. Acceptable Use - The proper and appropriate use of the University’s Electronic Resources in support of the teaching, learning, research and service missions of the University.

2. Access Control - The mechanism for limiting access to Information Resources to those users who are entitled to them.¹

3. Availability - Ensuring timely and reliable access to and use of information; The loss of availability is the disruption of access to or use of information or an information system.²

4. Confidential Information - Sensitive, high-risk information about an individual or the University including, but not limited to, student academic history, student discipline, student financial records, social security numbers, employment and benefit information, alumni giving, research information, user passwords, privileged communications, etc.

5. Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and personal information; the loss of confidentiality is the unauthorized disclosure of information.²

6. Data Classification - The conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted.³

7. Data Integrity - The correctness, completeness and validity of the information being maintained.

8. Data Steward - The individual responsible for the accuracy, integrity, consistency and relevancy of specific information within their assigned areas. The steward may be responsible for data managed and stored within a specific module of the Banner Enterprise Resource Planning (ERP) system, the Facilities database, the Library’s Millennium system, a Blackboard course site, the MySJU portal and its specific channel content, the University’s web sites and any other repository for University data.

9. Disaster Recovery - The ability of the University to respond to a disaster or an interruption of services by implementing a Disaster Recovery plan to stabilize and restore the critical functions.¹

¹ From SANS Institute http://www.sans.org/resources/glossary.php
10. Electronic Resources - This term includes, but is not limited to, the University’s hardware, software, desktop computers, laptops, operating systems, networks, servers, electronic mail services and other sources of electronic information.

11. Identity Management (IdM) - The management of user identities within the University and includes the management of roles and privileges assigned to users. IdM defines boundaries for the use of University electronic resources such as computers, software, operating systems, networks, electronic mail services, storage media, internet browsing and file transfer protocol.

12. Information Resources - Information in any form and recorded on any media, as well as all Electronic Resources.

13. Information Security - The safeguard of all Sensitive Information, electronic or otherwise, and the resources used to capture and manage that information.\(^4\)

14. Information Security Officer - The individual or individuals responsible for the oversight for Information Security at the University. The responsibility includes monitoring compliance with the University’s information security policies and procedures, making recommendations for improved security and monitoring the occurrence of Security Incidents. The Information Security Officers at the University are the Information Technology Executive Management team, which reports to the Vice President of Financial Affairs.

15. Integrity - The guarding against improper information modification or destruction, and includes ensuring information repudiation and authenticity; The *Loss of Integrity* is the unauthorized modification or destruction of information.\(^2\)

16. Internal Use Information - Information that requires some degree of protection and is specific to University operations including, but not limited to, internal memos, policies and correspondence.

17. Privacy - The freedom from unauthorized intrusion.\(^5\)

18. Security Incident - An event that occurs when an individual accesses an Information Resource in violation of this policy. The incident may impact or interrupt services, and in some cases may lead to disaster.\(^6\)

---


\(^5\) Merriam-Webster’s Dictionary definition

19. **Unit** - A University division, department, program, research center, service center or other operating unit.

20. **Unit Head** - The individual charged with the administrative responsibility for the Unit.

21. **Unrestricted Information** - Information that is generally available and open to the public including information found on the University external web sites such as faculty and staff names, titles, department information, work phones, class schedules, etc..

22. **User** - Any individual who accesses the University’s network services or Information Resources including students, faculty, staff, alumni and guests.

23. **Vulnerability** - A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system's security policy.\(^4\)