Mount St. Joseph University
Integrated Information Security Policy and Procedures

Policy Owners

OWNERSHIP	ROLE
Responsible	All Employees, Independent Contractors and Agents
Accountable	ISS Department Lead : Alex Nakonechnyi
Consulted	Management Team: Paige Ellerman, Whitney Kessinger, Alex Nakonechnyi

Revision History

DESCRIPTION	WRITTEN BY	REVISION DATE	APPROVED BY	APPROVAL DATE	EFFECTIVE DATE
Creation					
Update					

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE

This integrated information security policy and procedures (the “Policy” or “ISPP”) defines the administrative, technical, and physical safeguards (“Information Security Program”) in use at Mount St. Joseph University ("MSJ" or "Mount") in order to ensure the confidentiality, integrity, and availability of the data environment at MSJ. The Policy provides IT managers within MSJ with policies and guidelines concerning the acceptable use of MSJ Information Systems and Resources.

The Policy requirements and restrictions defined in this document shall apply to MSJ network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms.

This Policy must be followed by all MSJ Workforce Members, temporary workers, and all independent contractors working at the MSJ campus and telecommuting locations. This Policy shall be updated in response to environmental and operational changes affecting the security of MSJ information.

References: 16 C.F.R. §314.4 (e); ISO 5.1.

1.2 SCOPE

This Policy defines common security requirements for all MSJ personnel and systems that create, maintain, store, access, process or transmit MSJ information. This Policy also applies to Information Resources owned by others (such as contractors of MSJ), entities in the private sector, and in cases where MSJ has a legal, contractual, or fiduciary duty to protect said Resources while in MSJ custody. In the event of a conflict, the more restrictive measures shall apply. This Policy covers the MSJ network system which is comprised of various hardware, software, communication equipment, and other devices designed to assist MSJ in the creation, receipt, storage, processing, and transmission of MSJ information. MSJ’s network includes equipment connected to any MSJ domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by MSJ at its campus location or at remote locales.

The Policy is intended to set a minimum set of standards for information collection, sharing, storage, and processing at MSJ. Because different departments process data differently, each department is empowered to create their own policies and procedures to supplement this Policy in the event that more restrictive requirements are deemed necessary by a Supervisor. Departments are **not** authorized to deviate from the terms of this Policy in any

way that would result in a direct contradiction of, or relaxing of, the safeguards contained in this Policy.

1.3 ACRONYMS / DEFINITIONS

The following are key terms for use in this Policy. When capitalized in this Policy, the terms have the meaning shown below. Other notable terms shall be defined within the content of the Policy itself.

a. ***Information Resource or "Resource."*** Any MSJ-owned computer, workstation, smart phone, telephone, laptop, computer network, software, hardware, media, and Internet software and services that are intended for business use.

b. ***Information Security Policy and Procedures ("Policy" or "ISPP").*** This document, which establishes the basis for MSJ's Information Security Program.

c. ***Information Security Program.*** MSJ's enterprise-wide Information Security Program through which the administrative, technical, and physical safeguards required by this Policy are implemented, maintained, and audited.

d. ***Information System or "System."*** An interconnected set of Information Resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, information, data, applications, communications, and people.

e. ***ISS Department.*** Information Services and Support, responsible for information technologies support and related services.

f. ***ISS Department Lead.*** ISS Department Lead is responsible for confidentiality, integrity, and accessibility of all MSJ information.

g. ***Sensitive Information.*** MSJ information that requires safeguarding from unauthorized use or disclosure. Sensitive Information includes, but it not necessarily limited to student information, vendor confidential information, trade secrets, financial information, Social Security numbers, credit/debit card information, health-related information, background check information, or Workforce Member information.

h. ***Service Provider.*** A person or business that provides a service to MSJ directly involving covered accounts.

i. ***Supervisor***. A person responsible for overseeing and supervising the activities of a MSJ department or office.

j. ***User(s).*** Any Workforce Member authorized to access Information Systems and Resources.

k. ***Workforce Members.*** Employees and independent contractors of MSJ with assigned duties that involve the use of Sensitive Information in their performance of work for MSJ.

1.4 APPLICABLE STATUTES / REGULATIONS

The following is a list of laws, mandates, and regulations that were incorporated into the various policy statements included in this document.

a. Gramm Leach Bliley Act, 15 U.S.C. §6801, et. seq.

b. FTC "Red Flags Rule," 16 C.F.R. Part 681 Supplement A to Appendix A, 15 U.S.C. §1681m(e), et. Seq.

c. FTC "Safeguards Rule," 16 C.F.R. §314, et. seq.

d. NIST 800-53

e. NIST 800-171 ("NIST")

f. ISO/IEC 27001 ("ISO").

These laws and regulations serve as nationally and internationally recognized standards, which formally specify a management system intended to bring information security under explicit management control. While MSJ is not necessarily directly regulated by these laws or regulations, its clients may be so regulated and more broadly, these serve as foundational best practices for protecting information. Therefore, in support of its clients and in pursuing best practices, MSJ has implemented this Information Security Program and the Policy.

Reference: ISO 18.1.

1.5 ROLE OF ISS DEPARTMENT LEAD

Information technology services are governed by the ISS Department. The ISS Department Lead shall oversee all ongoing activities related to the development, implementation, and maintenance of MSJ information security policy and procedures in accordance with applicable federal and state laws, and any agreements. The current ISS Department Lead for MSJ is: Alex Nakonechnyi.

The ISS Department Lead and any designated or assigned personnel are responsible for maintaining a log of security enhancements and features that have been implemented to further protect all Sensitive Information and assets held by MSJ.

References: 16 C.F.R. §314.4 (a); ISO 5.1.2.

2. WORKFORCE MEMBER RESPONSIBILITIES

2.1 GENERAL REQUIREMENTS FOR WORKFORCE MEMBERS

The first line of defense in data security is the individual Workforce Member. Workforce Members are responsible for the security of all data which may come to them in whatever format. MSJ is responsible for maintaining ongoing training programs to inform all Users of these requirements. While this Policy includes numerous requirements that apply to Workforce Members (including Users) individually and collectively, the following are general security requirements that all Workforce Members are expected to follow. This list is not exhaustive, but intended as guidelines to put Workforce Members on notice.

a. Use Information Resources and Systems only for MSJ approved purposes and in accordance with MSJ Policy.

b. Secure Information Resources and Systems against unauthorized use, including keeping them physically secure when not in use and using all administrative, technical, and physical safeguards in accordance with this Policy.

c. Maintain and update User credentials, including strong passwords and other access controls to ensure access to Sensitive Information is limited to authorized personnel only.

d. Report all suspected or actual security incidents to the ISS Department Lead as required by this Policy.

e. Securely destroy all Sensitive Information and Information Resources.

f. Only use the minimum necessary Sensitive Information to accomplish any assigned duty.

g. Comply with all MSJ directions and notices concerning information security, to include applying all security patches and updates to MSJ Information Resources.

2.2 PROHIBITED ACTIVITIES

Workforce Members are prohibited from the following activities. The list is not exhaustive, but intended as a guideline to put Workforce Members on notice. Other prohibited activities are referenced elsewhere in this Policy.

a. Crashing an Information System. Deliberately crashing an Information System is strictly prohibited. If it is shown that the crash occurred as a result of User action, any repetition of the action by that User may be viewed as a deliberate act.

b. Attempting to break into an Information Resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other Resource permissions.

c. Introducing, or attempting to introduce malicious software, such as computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an Information System.

Exception: Authorized Information System support personnel, or others authorized by the ISS Department Lead, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection. For more information about MSJ's policies with respect to Peer-to-Peer sharing, please refer to the Peer-to-Peer (P2P) File Sharing Policy

d. Browsing. The willful, unauthorized access or inspection of confidential or Sensitive Information to which a Workforce Member has not been approved on a "need to know" basis is prohibited. MSJ has access to Sensitive Information, which includes personally identifiable information which is protected by laws and agreements which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which one has not been granted access by the appropriate approval procedure is strictly prohibited.

e. Personal or Unauthorized Software. Use of personal software on Information Resources without the express written approval of the ISS Department Lead is prohibited.

f. Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by MSJ is strictly prohibited.

g. System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures, or business interests of MSJ is strictly prohibited.

References: ISO 8.1.3; NIST 800-171 3.1.2, 3.4.9, 3.14.7

2.3 ELECTRONIC COMMUNICATION, E-MAIL, INTERNET USAGE

As a productivity enhancement tool, MSJ encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by MSJ-owned equipment are considered the property of MSJ and not the property of the individual User. Consequently, this Policy applies to all MSJ Workforce Members, contractors, and Users, and also covers all electronic communications including, but not limited to, those communications sent via telephones, e-mail, voicemail, instant messaging,

text/SMS messaging, Internet, fax, personal computers, mobile devices, and servers.

Information Resources, such as individual computer workstations, smart phones, laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

a. it does not consume more than a trivial amount of the Workforce Member's time or resources,

b. it does not interfere with staff productivity,

c. it does not preempt any MSJ activity,

d. it does not violate any of the following Policy requirements:

i. Copyright Violations. This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.

ii. Illegal Activities and Sports Pools. Use of Information Systems for or in support of illegal purposes as defined by federal, state, or local law is strictly prohibited. MSJ Information Systems shall not be used for operating or participating in sports pools.

iii. Commercial and Charitable Use. Use of Information Systems for personal or commercial profit is strictly prohibited. For example, Users may not use Information Systems for participating in offers to buy, sell, give away, or donate personal goods or services. Solicitation of charitable donations is also prohibited, unless otherwise approved by MSJ (such as United Way or Fine Arts Fund campaigns).

iv. Political Activities. All political activities are strictly prohibited on MSJ premises or through the use of Information Systems. MSJ encourages all of its Workforce Members to vote and to participate in the election process, but these activities must not be performed using Information Systems except as explicitly authorized by MSJ. Discussion of political issues and candidates, via Information Systems, is also inappropriate.

v. Social Media Use. Although social media use on Information Resources may be appropriate in some instances, Users must abide by the Social Media Guidelines.

vi. Harassment. MSJ strives to maintain a workplace free of harassment and that is sensitive to the diversity of its Workforce Members. Therefore, MSJ prohibits the use of Information Systems in ways that are disruptive, offensive to others, or harmful to morale.

vii. Junk E-mail. All communications using Information Systems shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, unauthorized solicitations, or other mass emails using a listserv, is prohibited, unless authorized by a Supervisor or the ISS Department. Any approved use of such "junk" mail shall be used responsibly and within the scope of the approved use.

- A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons.
- Advertisements offer services from someone else to a Workforce Member.
- Solicitations are when someone asks a Workforce Member for something.

If a Workforce Member receives any of the above on a MSJ workstation, device, or account, the Workforce Member shall delete the e-mail message immediately and report the message to the ISS Department Lead. Workforce Members shall not forward such e-mail messages to anyone or click on any links in such messages.

In addition to prohibiting the use of Information Systems for personal use, MSJ also prohibits the use of personal information systems and e-mail accounts for MSJ-related business or affairs. Workforce Members shall not use third party personal information services, such as Google Drive, Box.com, Dropbox, or personal e-mail without the explicit and written authorization of the ISS Department Lead.

Users should have no expectation of privacy in the use of Information Systems. Generally, while it is not the policy of MSJ to monitor the content of any electronic communication, MSJ is responsible for servicing and protecting MSJ's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. MSJ reserves the right, at its discretion, to review any Workforce Member's files or electronic communications to the extent necessary to ensure compliance with all applicable laws and regulations as well as MSJ policies. Workforce Members should compose all electronic communication with recognition of the fact that any content could be monitored, and that any electronic communication could be forwarded, intercepted, printed, or stored by others.

References: NIST 800-171 3.1.2, 3.13.1

2.4 INTERNET ACCESS

Internet access is provided for MSJ Users and is considered a great resource for MSJ. This Resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative, or contract needs. The Internet access provided by MSJ should not be used for personal purposes or entertainment, such as listening to online radio, watching movies or videos, or playing games.

Users must understand that individual Internet usage is monitored, and if a Workforce Member is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action may be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and online music sharing applications, have already been blocked by MSJ routers and firewalls. This list of unacceptable websites is constantly monitored and updated as necessary. Any User visiting pornographic websites will be disciplined and may be terminated. In the event that a User must visit an unacceptable website for legitimate research, academic, or MSJ-related work, that User must receive explicit approval in writing by the ISS Director Lead and General Counsel.

Reference: NIST 800-171 3.1.2

2.5 REPORTING SOFTWARE OR HARDWARE MALFUNCTIONS

Users should immediately inform the appropriate MSJ personnel when the User's hardware or software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk or may be symptomatic of a larger issue. If the User, or the User's manager or Supervisor, suspects a computer virus infection, it should be reported to the ISS Department Lead and the following steps should be taken immediately:

a. Stop using the computer.

b. Do not carry out any commands, including commands to <Save> data.

c. Do not close any of the computer's windows or programs.

d. Do not turn off the computer or peripheral devices.

e. If possible, physically disconnect the computer from any networks to which it is attached.

f. Inform the appropriate personnel or ISS Department Lead as soon as possible. Write down any unusual activity of the computer or Information Resource (screen messages, unexpected disk access,

unusual responses to commands) and the date/time when these activities were first noticed.

g. Write down any changes in hardware, software, or use of software that preceded the malfunction.

h. Do not attempt to remove a suspected virus or malicious software.

The ISS Department Lead should monitor the resolution of the malfunction or incident, and record the result of the action with recommendations on action steps to avoid similar occurrences in the future.

References: ISO 16.1; NIST 800-171 3.14.1

2.6 REPORT SECURITY INCIDENTS

It is the responsibility of every Workforce Member and User to report actual or suspected security incidents on a continuous basis to the appropriate Supervisor or ISS Department Lead. Users are responsible for the day-to-day, hands-on security of any Information Resources assigned to him or her.

Workforce Members are expected to formally report all security incidents to either their immediate Supervisor, or to the ISS Department Lead, through the established procedure. Reports of security incidents shall be escalated as quickly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated and taken shall be documented. It is the responsibility of the ISS Department Lead to provide training on any procedural changes that may be required as a result of the investigation of the incident.

Any incidents that involve a potential compromise of Sensitive Information must be escalated to the ISS Department Lead and managed in strict accordance with legal counsel and the Incident Response Plan.

References: 16 C.F.R. §314.4 (c); ISO 16.1.2; NIST SP 800-53 Rev. 4 IR-6, SI-5; NIST 800-171 3.6.2, 3.14.3

2.7 TRANSFER OF SENSITIVE INFORMATION

When Sensitive Information sent from one individual is received by another individual while conducting MSJ business, the receiving individual shall maintain the confidentiality of the information in accordance with the conditions imposed by the providing individual. All Workforce Members must recognize the sensitive nature of data maintained by MSJ and hold all data in the strictest confidence. Any purposeful and unauthorized release of Sensitive Information by a Workforce Member may result in disciplinary action, up to and including, termination of employment or a contract.

References: ISO 13.2.1.

2.8 TRANSFERRING SOFTWARE & FILES BETWEEN COMPANY AND PERSONAL DEVICES

Personal software shall not be used on Information Resources or Information Systems unless approved in writing by the ISS Department Lead. MSJ's Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Personal software and the use of personal computing devices on Information Resources or networks can compromise the security protections in use.

If a need for specific software exists, Users shall submit a request to the applicable Supervisor. Users shall not use MSJ purchased software on non-Information Resources. Sensitive Information shall not be placed on any computer that is not the property of MSJ without written consent of the ISS Department Lead. In the event that a Supervisor receives a request to transfer MSJ data to a non-MSJ Computer System, the Supervisor should notify the ISS Department Lead or appropriate personnel of the intentions and the need for such a transfer of data.

2.9 INTERNET CONSIDERATIONS

Special precautions are required to block Internet (public) access to Information Resources not intended for public access, and to protect Sensitive Information when it is to be transmitted over the Internet.

The following guidelines shall govern Internet usage.
Prior approval of the ISS Department Lead or appropriate personnel authorized by MSJ shall be obtained before:

a. A new Internet, or other external network connection, is established;

b. MSJ information (including notices, memoranda, documentation and software) is made available on any Internet-accessible Information Resource (e.g. web or ftp server); or

c. Sensitive information, including credit card numbers, account numbers, data subject names, and identifiable information shall always be encrypted before being transmitted through the Internet.

References: NIST SP 800-53 Rev. 4 SC-7; NIST 800-171 3.13.5; (all of Section 2).

3. IDENTIFICATION AND AUTHENTICATION

3.1 USER LOGIN IDS

Individual Users shall have unique login IDs. An access control system shall identify each User and prevent unauthorized Users from entering or using

Information Resources. The following requirements shall be satisfied in the establishment and maintenance of User login IDs and passwords.

a. Each User shall be assigned a unique identifier.

b. Users shall be responsible for the use and misuse of their individual login ID.

c. All User login IDs shall be audited at least twice yearly and all inactive login IDs shall be revoked.

d. Users who desire to obtain access to Information Systems must have a completed and signed a New Hire/New Volunteer Form (the "Network Access Form"). This form must be signed by the Supervisor of each User requesting access.

References: 16 C.F.R. 314.4 (b)(3); ISO 9.2; NIST SP 800-53 Rev. 4 AC-2, IA-2, IA-8; NIST 800-171 3.1.1, 3.1.7, 3.5.1, 3.5.6.

3.2 PASSWORDS AND USER AUTHENTICATION

a. User Account Passwords. User Login IDs and passwords are required in order to gain access to all Information Systems and Information Resources.

b. Password Generation and Initial Access. Users are required to select a password or other credential in order to obtain access to any electronic information both at the Information System and Information Resource level. When passwords are reset, the User will be automatically prompted to manually change that randomly assigned password to his or her own password. The ISS Department Lead shall not and will not have access to or maintain a record of User passwords.

c. Password Requirements. Passwords are required to be a minimum of ten characters. Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters (such as digits 0-9), and special characters (such as !, $, #, %). Further, passwords must not contain the User's account name or parts of the User's full name that exceed two consecutive characters.

d. User Password Security. Users shall not share passwords with anyone, including personal assistants, colleagues, or family members. While Users are discouraged from writing down passwords, any documents containing passwords must be kept secure in a locked drawer or other physically secure location. **The ISS Department Help Desk will never ask for your password**.

e. MSJ Password Security. When possible, passwords shall be masked or suppressed on all online screens, and shall never be

printed or included in reports or logs. Passwords shall be stored in encrypted format and not in plain text.

f. Password Changes. A User should change his or her password any time the User believes the password has been compromised. At a minimum, passwords should be changed every one hundred twenty (120) days.

g. Password Re-Use. MSJ systems shall be configured to prevent the re-use of the past five (5) passwords for any User.

h. Other Authentication Measures. Nothing in this Policy prohibits MSJ from pursuing and implementing additional authentication measures, including multi-factor authentication.

References: 16 C.F.R. §314.4 (b)(1); ISO 9.2.4, ISO 9.3; NIST SP 800-53 Rev. 4 AC-2, IA-3, IA-4; NIST 800-171 3.5.2, 3.5.3, 3.5.5, 3.5.7, 3.5.8, 3.5.10, 3.5.11.

3.3 ACCESS AUTHORIZATION

Workforce Members shall be granted access to Sensitive Information and Information Systems in accordance with their assigned work duties. In other words, Workforce Members access to Sensitive Information should be on a "need to know basis." To meet this requirement, MSJ shall implement access controls to ensure that Workforce Member access is assigned, maintained, and terminated accordingly.

Supervisors shall be responsible for determining access requirements for any Workforce Members in their department. Rules for access to Information Systems (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the Resources.

Access to Information Systems is granted only by the completion of a Network Access Form. This form can only be initiated by the appropriate Supervisor, and must be signed by the Supervisor and the ISS Department Lead.

References: 16 C.F.R. §314.4 (b)(2); ISO 9.1.1, ISO 9.2.2; NIST SP 800-53 Rev. 4 AC-3, AC-5, AC-19, AC-20, AC-21, IA-3, IA-5; NIST 800-171 3.1.4, 3.13.3.

3.4 USER LOGIN ENTITLEMENT REVIEWS

If a Workforce Member changes positions at MSJ, the Workforce Member's new Supervisor shall promptly notate the change of roles by indicating on the Network Access Form both the roles or access that need to be added and the roles or access that need to be removed so that Workforce Member has access to the minimum necessary data to effectively perform their new job functions. The effective date of the position change should also be noted on the Form so that MSJ can ensure that the Workforce Member will have appropriate roles, access,

and applications for their new job responsibilities. For a limited training period, it may be necessary for the Workforce Member who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new job responsibilities.

No less than annually, departments shall, if there have been any entitlement or access changes, request meetings with the ISS Department to facilitate entitlement reviews with Supervisors to ensure that all Workforce Members have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary data.

References: 16 C.F.R. § 314.4 (b)(2); ISO 9.2.3, ISO 9.2.5, ISO 9.2.6; NIST SP 800-53 Rev. 4 IA-5, IA-6.

3.5 TERMINATION OF WORKFORCE MEMBER AND USER LOGON ACCOUNT

Upon termination of a Workforce Member, whether voluntary or involuntary, the Workforce Member's Supervisor shall promptly notify management and ISS Department Lead by completing a Network Termination Form ("Network Termination Form") and submitting the Network Termination Form to the ISS Department Lead. If the Workforce Member's termination is voluntary and the Workforce Member provides notice, the Workforce Member's Supervisor shall promptly notify ISS Department Lead of the Workforce Member's last scheduled work day so that their User account(s) can be configured to expire. The Workforce Member's Supervisor shall be responsible for insuring that all keys, ID badges, and other access credentials as well as MSJ equipment and property is returned to MSJ. All such materials must be returned prior to the Workforce Member leaving MSJ on their final day of employment, or the last day of any contract.

No less than quarterly, the ISS Department Lead or their designee shall provide a list of active User email accounts and User accounts for both network and application access to Supervisors for review. Department heads shall review the active email and access lists within five (5) business days of receipt. If any of the Workforce Members on the list are no longer employed or contracted by MSJ, the Supervisor will immediately notify ISS Department of the Workforce Member's termination status and submit the Network Termination Form.

References: 16 C.F.R. §314.4(b)(3); ISO 9.2.6; NIST SP 800-53 Rev. 4 IA-2, IA-4, IA-10, PS-4.

3.6 LOG-IN MONITORING

MSJ shall install the necessary technical and administrative safeguards to properly monitor all attempted and actual log-ins to Information Systems. The ISS Department Lead is responsible for the implementation of such safeguards and regular auditing of such log reports to properly identify and remedy unauthorized access or attempts at such access.

References: 16 C.F.R. §314.4 (b)(1); ISO 12.4; NIST SP 800-53 Rev. 4 IA-10.

3.7 DATA SUBJECT REQUESTS

MSJ may maintain and process personally identifiable information relating to individuals from around the world. In certain jurisdictions, data subjects have the right to request MSJ take particular actions with respect to the data subject's personal data, including furnishing copies and erasure. Any Workforce Member responsible for fielding and responding to data subject requests must make every effort to authenticate the data subject's identity prior to processing or honoring the request, while also confirming that the data subject is eligible for making the request at issue. MSJ should authenticate the data subject's identity by requesting confirmation of data elements already in MSJ's possession. Under no circumstances should MSJ seek to authenticate a data subject's identity by requesting personal data not already in MSJ's possession.

With respect to "Student Records," as that term is defined under FERPA, Workforce Members should refer to FERPA Guidelines for Employees for additional guidance.

3.8 AUTOMATIC LOG OFF

MSJ shall implement technical measures to force or compel the logging off of Information Systems containing Sensitive Information due to fifteen (15) minutes of inactivity.

References: 16 C.F.R. §314.4 (b)(3); NIST SP 800-53 Rev. 4 IA-3.8; NIST 800-171 3.1.10, 3.1.11.

4. NETWORK CONNECTIVITY

4.1 NETWORK CONNECTIONS AND REMOTE ACCESS

General Access. All Workforce Member access to Information Systems shall be requested and approved using the Network Access Form. No exceptions. With the approval of such access in place, Workforce Members shall work with the appropriate ISS Department resources to establish and maintain network access in accordance with this Policy.

References: ISO 9.1.2, ISO 13.1.1; NIST SP 800-53 Rev. 4 3.1.12, 3.13.5.

Any systems that allow public access to host computers, including mission-critical servers, warrant additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

References: ISO 12.4.

Remote Access. Remote access to Information Systems shall be subject to authorization and authentication by an access control system and protected via a virtual private network ("VPN"). The ISS Department Lead shall establish and supervise such access control systems. Remote access privileges are granted only upon the request of a Supervisor with the submission of the Network Access Form and the approval of the ISS Department Lead or appropriate personnel. All remote access should also be secure via enabled multi-factor authentication.

References: ISO 6.2.2; NIST SP 800-53 Rev. 4 AC-17; NIST 800-171 3.1.12, 3.1.14, 3.1.16, 3.1.18.

4.2 OUTBOUND CONNECTIONS

MSJ provides Users a link to an Internet Service Provider. If a User has a specific need to link with an outside computer or network through a direct link, prior approval must be obtained from the ISS Department Lead. The ISS Department Lead or designated IT Department personnel will ensure adequate security measures are in place.

References: ISO 13.1; NIST SP 800-53 Rev. 4 SC-7

4.3 THIRD-PARTY CONNECTIONS

The security of Information Systems can be jeopardized from third-party locations if security practices and Resources are inadequate. When there is a need to connect to a third-party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of MSJ Information System. The ISS Department Lead or appropriate personnel should be involved in the design and approval of any such connection.

References: ISO 13.1; NIST SP 800-53 Rev. 4 SC-7.

4.4 SECURITY IN THIRD-PARTY CONTRACTS

Access to a MSJ Information System should not be granted until a review of the following issues and requirements have been made.

a. Applicable sections of this Policy have been reviewed and considered.

b. Policies and standards established in the ISPP have been enforced.

c. A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.

d. The right to audit contractual responsibilities are included in the agreement.

e. Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the legal and contractual obligations to MSJ clients and any regulators.

f. A description of each service to be made available.

g. Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.

h. A detailed list of Users that have access to the MSJ Information System must be maintained and auditable.

i. If required under the contract, permission should be sought to screen authorized Users.

j. Dates and times when the service is to be available should be agreed upon in advance.

k. Procedures regarding protection of Information Resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.

l. The right to monitor and revoke third-party user activity should be included in each agreement.

m. Language on restrictions on copying and disclosing Sensitive Information should be included in all agreements.

n. Responsibilities regarding hardware and software installation and maintenance should be understood and agreed upon in advance.

o. Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.

p. If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.

q. A formal method to grant and authorize Users that will have access to the data collected under the agreement should be formally established before any Users are granted access.

r. Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.

s. Mandating annual security training on the ISPP, including a formal procedure to ensure that the training takes place, is attended by all required Users, and that the content is appropriate to support this MSJ Policy and others.

t. A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement being entered.

References: ISO 12.5; NIST SP 800-53 Rev. 4 PS-7, SA-9.

4.5 FIREWALLS

MSJ authorization by the ISS Department Lead must be received before any User is granted direct access to a MSJ router or firewall, if ever.

References: 16 C.F.R. §314.4 (d) (1) & (2); §314.4 (b)(3); ISO 12.5; NIST SP 800-53 Rev. 4 SC-7.

5. MALICIOUS CODE AND OTHER SOFTWARE

5.1 NEW SOFTWARE DISTRIBUTION

All new software will be tested by the IT Department in order to ensure compatibility with currently installed software and network configuration. In addition, all Users must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from the Internet, or on disks.

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the ISS Department Lead. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Information Resources/Information Systems. These precautions include determining that the software does not interfere with or damage MSJ hardware, software, or data, and that the software does not contain viruses, either originating with the software or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a MSJ Information System/Information Resource from another location must be scanned for viruses immediately after being received and before being released to Users.

All portable media is a potential source for a computer virus. Therefore, every CD-ROM, DVD, and USB device must be scanned for virus infection prior to copying information to a MSJ Information System/Information Resource.

Computers shall never be “booted” from portable media (CD-ROM, DVD, or USB device) received from an outside source. Users shall always remove any portable media device from the computer when not in use. This is to ensure that the portable media device is not in the computer when the machine is powered on. A portable media device infected with a boot virus may infect a computer in that manner, even if the portable media device is not “bootable.”

References: ISO 12.2, ISO 12.6; NIST SP 800-53 Rev. 4 CM-10, SA-4, SI-3; NIST 800-171 3.7.4, 3.14.2

5.2 RETENTION OF OWNERSHIP

All software programs and documentation generated or provided by Workforce Members for the benefit of MSJ are the property of MSJ unless otherwise addressed by a contractual agreement. Workforce Members developing programs or documentation must sign a statement acknowledging MSJ ownership at the time of employment or care.

Reference: ISO 8.1.2

6. ENCRYPTION

6.1 GENERAL POLICY

Encryption is the most effective way to achieve data security by rendering Sensitive Information unreadable or usable without access to the decryption key. Whenever possible and feasible, MSJ requires that all Sensitive Information be encrypted, in transit and at rest. All MSJ-issued laptops and mobile devices shall be encrypted and shall transmit all Sensitive Information in an encrypted format.

6.2 INSTALLATION OF AUTHENTICATION AND ENCRYPTION CERTIFICATES ON THE E-MAIL SYSTEM

Any User desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user by contacting the ISS Department Lead. Once verified, the certificate is installed on each recipient workstation, and the two may safely exchange secure e-mail. Approved secure e-mail solutions are also an option.

6.3 FILE TRANSFER PROTOCOL (FTP)

Files may be transferred to secure FTP websites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the ISS Department Lead or ISS Department.

6.4 SECURE SOCKET LAYER (SSL) WEB INTERFACE

If access to an external website is required for any Information System storing Sensitive Information, the connection must be made via a secure SSL or TSL managed website. Any such access must be requested using the Network Access Form.

References: 16 C.F.R. §314.4 (b)(3); ISO 10; NIST SP 800-53 Rev. 4 SC-8, SC-13, SC-28; NIST 800-171 3.1.13, 3.1.17, 3.13.4. 3.13.10.

7. PHYSICAL AND BUILDING SECURITY

It is the Policy of MSJ to provide building access in a secure manner. Each MSJ building, may be somewhat unique in terms of layout, entranceway access, fire escape requirements, and server room control. However, MSJ strives to continuously upgrade and expand its security and to enhance protection of its assets and MSJ information. The following are the minimum requirements for the physical security of any facility, office, or location in which Information Systems and Sensitive Information are stored.

a. Each MSJ building/department will adopt a security plan, which includes identification and location of Information Systems and Sensitive Information.

b. Entrance to MSJ buildings during non-working hours shall be access-controlled through the use of physical locks or other key systems to which only authorized personnel have access.

c. Workforce Members shall immediately report any lost or stolen access credentials or keys to their Supervisor and ISS Department Lead as soon as possible.

d. Where possible, facilities should be safeguarded by an alarm system which notifies campus police.

e. Any unmonitored door with access to spaces where Sensitive Information is in use, must remain locked.

f. The reception area shall be staffed at all times during normal working hours.

g. Any unrecognized person in a restricted office location should be challenged as to their right to be there. If for any reason Workforce Members have concerns about such a challenge, they should report any unrecognized persons to their Supervisor or campus police.

h. All Workforce Members shall follow the relevant Residence Life Policy in the Student Handbook. Additionally, all dormitory overnight visitors must sign in at the front desk and provide contact information in case of emergency.

i. Fire Protection. Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

j. Maintenance Records. Any maintenance performed on MSJ facility security systems, or on the building itself, to the extent it could impact physical security must be documented. Such maintenance records must be maintained by the ISS Department Lead for six (6) years unless otherwise approved by Chief Compliance and Risk Officer.

k. Office, workspace and workstation security.

i. **Workforce Members shall lock offices, cabinets, drawers, and any other storage spaces containing, or allowing access to, Sensitive Information when not in use. If not possible, Workforce Members shall have such offices, cabinets, drawers, and any other storage spaces secured behind locked doors or be attended to when not secured.**

ii. Workstations that store or access Sensitive Information shall only be in access-controlled locations. Laptops and mobile devices with access to Sensitive Information shall remain physically secure or under Workforce Member control at all times. Any loss or theft of a device containing or capable of accessing Sensitive Information or Information Systems should be reported to the ISS Department Lead immediately.

iii. Workstations accessing and displaying Sensitive Information shall be located in rooms accessible only by personnel authorized to use Sensitive Information and shall be oriented as to most effectively minimize incidental viewing by individuals without authorization to view Sensitive Information. For example, workstation monitors with Sensitive Information should face away from hallways and publicly accessible areas.

iv. Workforce Members shall log off any Information Systems and Information Resource when completing assigned tasks.

v. When possible, Workforce Members shall activate locking workstation and laptop screen savers that prohibit access without the entry of a password.

References: 16 C.F.R. §314.4 (b)(3); §314.4 (c); ISO 11; NIST SP 800-53 Rev. 4 PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-13, PE-16, PE-18, PE-20; NIST 800-171 3.10.1, 3.10.2, 3.10.3, 3.10.5.

8. WORKING REMOTELY ("TELECOMMUTING")

MSJ considers working remotely ("telecommuting") to be an acceptable work arrangement in certain circumstances and only with explicit MSJ approval. This Policy is applicable to all Workforce Members who work either permanently or only occasionally outside of the MSJ office environment. It applies to Workforce Members who work from their home full-time, Workforce Members on temporary travel, Users who work from a satellite office location, and to any User who connects to a MSJ network from a remote location.

While telecommuting can be an advantage for Workforce Members and for MSJ in general, it presents new risks in the areas of confidentiality and security of data. Workforce Members linked to MSJ's network become an extension of the WAN and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes MSJ's Sensitive Information to risks not present in the traditional office environment.

Reference: ISO 6.2.2

8.1 GENERAL REQUIREMENTS

Telecommuting Users are required to follow all policies that are applicable to other Workforce Members. Failure to follow any of these policies or information security requirements while working remotely may be grounds for disciplinary action, including termination.

8.2 REQUIRED EQUIPMENT

Workforce Members approved for telecommuting must understand that MSJ will not provide all equipment necessary to ensure proper protection of information to which the Workforce Member has access; however, the minimum equipment and environment required is addressed in the MSJ Flex Work Schedule and Telecommuting policy.

Reference: ISO 8.1.2

8.3 HARDWARE SECURITY PROTECTIONS

a. Virus Protection. Remote Users must never stop the update process for virus protection. Virus protection software is installed on all MSJ computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete.

b. VPN and Firewall Use. Established procedures must be rigidly followed when accessing MSJ information of any type. MSJ requires the use of VPN software and a firewall device for remote access. Disabling a firewall or failing to use a VPN is reason for termination.

c. Physical Security. Remote Users must maintain the physical security of all Information Resources, either by direct physical control or the use of lockable storage units or offices. If such portable devices must be left in a car, they should be stored in a locked trunk and out of sight.

d. Multi-factor Authentication. Multi-factor authentication for devices connecting remotely should be enabled and in use.

e. Lock Screens. No matter what location, Users shall lock the screen before walking away from the workstation or laptop. Users shall ensure the activation of any automatic log-off feature to log the portable device out after a set period of inactivity.

Reference: ISO 11.2.6; NIST 800-171 3.1.10.

8.4 DATA SECURITY PROTECTION

a. Data Backup. Remote Users shall follow established backup procedures for all data, to include storing such backups on MSJ networks and using all available encryption technology. Remote Users shall not create separate backups locally on any Information Resource.

b. Transferring Data to and from MSJ. Transferring of data to MSJ requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted.

c. E-mail. Encryption should be considered when sending Sensitive Information. Personal e-mail accounts shall never be used for MSJ business.

d. Non-MSJ Networks. Extreme care must be taken when connecting MSJ equipment to a home, hotel, or public network. All such connections shall be made with MSJ VPN in use. MSJ has no ability to monitor or control the security procedures on non-MSJ networks.

e. Hard Copy Reports or Documents. All MSJ documents should be secured when not in use. Workforce Members shall not leave such documents out in public view. All MSJ documents should be securely shredded prior to recycling or disposal.

f. Data Entry When in a Public Location. Workforce Members are expected to use care and discretion when working in a public location. Workforce Members should not perform work tasks which require the use of Sensitive Information when easily observed in a public area (i.e. airports, airplanes, hotel lobbies, coffee shops).

g. Sending Sensitive Information Outside MSJ. All external transfer of data must be associated with an official MSJ contract, non-disclosure agreement, or other written agreement in which the recipient is bound to protect Sensitive Information. Sensitive Information must be transmitted through secure, encrypted, means.

8.5 DISPOSAL OF PAPER AND/OR EXTERNAL MEDIA

a. Shredding. All paper which contains Sensitive Information that is no longer needed must be shredded or otherwise rendered unreadable

before being discarded or recycled. Workforce Members shall not place such paper in a trash container or recycle bin without first shredding. All Workforce Members permanently working remotely MUST have direct access to a shredder.

b. Disposal of Electronic Media. All electronic media must be disposed of in accordance with this Policy and in the same manner as would take place should the Workforce Member work in a MSJ office.

Reference: ISO 8.3.2; NIST 800-171 3.8.3.

9. SPECIFIC PROTOCOLS AND DEVICES

9.1 WIRELESS USAGE STANDARDS AND POLICY

This Policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of MSJ Information Resources using wireless networks. Any wireless use will be approved by the ISS Department Lead prior to implementation.

In order to be granted the ability to utilize the wireless network interface on any Information Resource, Workforce Members shall be required to obtain the approval of their immediate Supervisor and the ISS Department Lead. The Network Access Form is used to make such a request.

The ISS Department Lead shall establish the minimum software and security requirements for any wireless access. Where provided, multi-factor authentication must be utilized to gain access to any Information Resource.

Reference: NIST SP 800-53 Rev. 4 AC-18; NIST 800-171 3.1.16, 3.1.17.

9.2 USE OF PORTABLE MEDIA

The use of portable media in various formats is not common practice within MSJ. All Users must be aware that Sensitive Information could potentially be lost or compromised when moved outside of MSJ networks. Portable media received from an external source could potentially pose a threat to MSJ networks. Portable media within the scope of this Policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB “thumb” or “flash” drives. Since portable media are easily lost, care and protection of these devices must be addressed. In the rare cases portable media use is required the following rules must be followed.

MSJ rules governing the use of portable media include:

a. No Sensitive Information should ever be stored on portable media unencrypted.

b. All portable media used to store Sensitive Information must be issued and tracked by MSJ. Workforce Members shall not use personal portable media to store Sensitive Information.

c. Users must never connect their MSJ-owned portable media device to a workstation or device that is not issued by MSJ. Non-MSJ workstations and laptops may not have the same security protection standards required by MSJ. Therefore, virus patterns could potentially be transferred from the non-MSJ device to the media and then back to the MSJ workstation.

d. Before initial use and before any Sensitive Information may be transferred to portable media, any portable media must be sent to the ISS Department Lead to ensure approved encryption is used.

e. Workforce Members must report the loss or theft of all MSJ portable media to their immediate Supervisor. It is important that the ISS Department Lead is notified either directly from the Workforce Member or by the Supervisor immediately.

f. When a Workforce Member leaves MSJ, all MSJ portable media in his or her possession must be returned to the ISS Department Lead or ISS Department for secure data erasure in accordance with this Policy.

References: 16 C.F.R. §314.4 (c); ISO 8.3.1; NIST SP 800-53 Rev. 4 MP-2, MP-5, MP-6, MP-7; NIST 800-171 3.8.7, 3.8.8.

10. RETENTION / DESTRUCTION OF COMPANY INFORMATION

Many MSJ contracts, as well as state and federal laws, require MSJ to retain, return or destroy information for various reasons. For example, as an academic institution, FERPA mandates that educational records be preserved to enable students and former students to exercise rights with respect to access to that information. Please refer to the Record Retention and Document Destruction Policy for further guidance, and the MSJ Records Retention Schedule for specific guidance on retention requirements for various types of data and documents.

Record Destruction. All hard copy MSJ records that require destruction are to be securely shredded using commercially reasonable and industry standards.

The ISS Department Lead and Chief Compliance and Risk Officer shall determine the proper retention periods and the method for destruction of MSJ records and documenting such destruction.

References: 16 C.F.R. §314.4 (c).

11. HARDWARE AND ELECTRONIC MEDIA TRACKING; DISPOSAL

11.1 ACCOUNTABILITY

During normal operations and when responding to an incident, it is critical that MSJ can quickly and properly determine the hardware and media in its inventory. MSJ shall implement procedures by which MSJ hardware and electronic media used to store Sensitive Information is properly acquired, maintained, transferred, and destroyed. The ISS Department Lead is responsible for implementing a procedure which includes documentation that logs all such MSJ hardware through their lifecycle at MSJ. Such logs shall be retained for a period of no less than six (6) years for purposes of audit, unless otherwise stipulated by policy, contract or law.

References: ISO 8.1.1; NIST SP 800-53 Rev. 4 CM-8, SA-4; NIST 800-171 3.4.1.

11.2 DISPOSAL OF EXTERNAL MEDIA

It must be assumed that any external media in the possession of a Workforce Member is likely to contain Sensitive Information. Accordingly, external media (CD-ROMs, DVDs, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

All media will be secured until securely destroyed in accordance with this Policy. It is the responsibility of each Workforce Member to identify media which should be destroyed and to utilize this Policy in its destruction. When no longer needed all forms of external media are to be sent to the ISS Department Lead for proper disposal. External media should never be thrown in the trash.
References: ISO 8.3.2; NIST SP 800-53 Rev. 4 MP-6.

11.3 DISPOSAL OF HARDWARE

All hardware scheduled for disposal will be wiped of all data, and all MSJ settings and configurations will be reset to factory defaults. No other settings, configurations, software installation, or options will be made. Asset tags and any other identifying logos or markings will be removed.

References: 16 C.F.R. §314.4 (c); ISO 11.2.7; NIST SP 800-53 Rev. 4 MP-6

12. CHANGE MANAGEMENT

STATEMENT OF POLICY

MSJ must be able to trust all changes to Information Systems and Information Resources including software releases and software vulnerability patching in Information Systems that contain Sensitive Information. Change tracking allows the ISS Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the System.

PROCEDURE

a. The ISS Department shall carefully log all changes made to any Information System or Information Resource.

   i. When changes are tracked within a system, such as Windows updates in the Add or Remove Programs component or system updates performed and logged by a vendor, these changes do not need to be logged on the change management tracking log; however, the Workforce Member implementing the change will ensure that the change tracking is available for review, if necessary.

b. The ISS Workforce Member implementing the change will ensure that all necessary data backups are performed prior to the change.

c. The ISS Workforce Member implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the System or Resource and needs to be removed.

References: ISO 12.1.2; NIST SP 800-53 Rev. 4 CM-3, CM-4, CM-5; NIST 800-171 3.4.5

13. AUDIT CONTROLS

STATEMENT OF POLICY

MSJ shall implement hardware, software, and/or procedural mechanisms that record and examine activity in Information Systems that contain Sensitive Information. Audit Controls are technical mechanisms that track and record computer activities. An audit trail may determine if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or User activities.

MSJ is committed to routinely auditing Users' activities in order to continually assess potential risks and vulnerabilities to Sensitive Information in its possession. As such, MSJ will continually assess potential risks and vulnerabilities to Sensitive Information in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the law and industry best practices.

PROCEDURE

a. See policy entitled Information System Activity for the administrative safeguards for auditing system activities.

b. MSJ shall enable event auditing on all computers that process, transmit, and/or store Sensitive Information for purposes of generating audit logs. Each audit log shall include, at a minimum: User ID, login time and date, and scope of Sensitive Information being accessed for each attempted access.

c. Audit trails shall be stored on a separate computer system to minimize the impact of such auditing on business operations and to minimize access to audit trails.

d. MSJ shall utilize appropriate network-based and host-based intrusion detection systems. The ISS Department Lead shall oversee the implementation and use of such systems.

References: 16 C.F.R. §314.4 (b)(3); ISO 12.7; NIST SP 800-53 Rev. 4 AU-1, AU-9, AU-11, AU-12, PM-14; NIST 800-171 3.3.1, 3.3.3, 3.3.8.

14. INFORMATION SYSTEM ACTIVITY REVIEW, RISK ASSESSMENT AND RISK MANAGEMENT

STATEMENT OF POLICY

The purpose of this Policy is to establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, User accounts, system access, file access, security incidents, audit logs, and access reports. MSJ shall conduct a regular internal review of records of system activity to minimize security violations. In conjunction with Information System Activity Reviews, MSJ shall regularly schedule and complete risk assessments and implement steps to mitigate any identified risks to information security.

Information System Activity Review

a. See policy entitled Audit Controls for a description of the technical mechanisms that track and record activities on Information Systems that contain or use Sensitive Information.

Reference: ISO 12.7

b. The ISS Department Lead shall be responsible for conducting reviews of Information Systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.

Reference: ISO 18.2

c. The ISS Department Lead shall develop a report format to capture the review findings. Such a report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, Workforce Member training and/or discipline, program adjustments, modifications to safeguards).

d. Such reviews shall be conducted annually. Audits also shall be conducted if MSJ has reason to suspect wrongdoing. In conducting these reviews, the ISS Department Lead shall examine audit logs

for security-significant events including, but not limited to, the following:

i. Logins. Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.

ii. File Accesses. Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.

iii. Security Incidents. Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.

iv. User Accounts. Review User accounts within all systems to ensure Users that no longer have a business need for Information Systems no longer have such access to the information and/or system.

References: ISO 9.2, ISO 18.2.3; NIST 800-171 3.13.3.

e. The ISS Department Lead shall be responsible for maintaining such System Activity Reports. The ISS Department Lead shall consider such reports and recommendations in determining whether to make changes to MSJ's administrative, physical, and technical safeguards.

References: NIST SP 800-53 Rev. 4 CA-2, MP-2, PM-9, PM-12, PM-14, RA-2, RA-3, SA-5, SI-5; NIST 800-171 3.3.5, 3.4.2, 3.7.1. 3.7.2, 3.11.1

15. DATA INTEGRITY

STATEMENT OF POLICY

MSJ shall implement and maintain appropriate electronic mechanisms to corroborate that Sensitive Information has not been altered or destroyed in an unauthorized manner. The purpose of this Policy is to protect MSJ's Sensitive Information from improper alteration or destruction.

PROCEDURE

a. To the fullest extent possible, MSJ shall utilize applications with built-in intelligence that will automatically check for human errors.

b. MSJ shall acquire appropriate network-based and host-based intrusion detection systems. The ISS Department Lead shall be responsible for overseeing the installing, maintaining, and updating such systems.

c. To prevent transmission errors as data passes from one computer to another, MSJ will use encryption, as determined to be appropriate, to preserve the integrity of data.

d. MSJ will check for possible duplication of data in its Information Systems and Resources to prevent poor data integration between different computer systems.

e. To prevent programming or software bugs, MSJ will test its Information Systems for accuracy and functionality before it starts to use them. MSJ will update its Systems in a timely fashion when IT vendors release fixes to address known bugs or problems.

f. MSJ will install and regularly update anti-virus software on all workstations to detect and prevent malicious code from altering or destroying data.

References: 16 C.F.R. §314.4 (b)(3); NIST SP 800-53 Rev. 4 PL-8, SC-7; NIST 800-171 3.6.1, 3.13.2, 3.13.3.

16. CONTINGENCY PLAN

STATEMENT OF POLICY

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, terrorism, hack, denial of service attack, system failure, and natural disaster) that damages systems that contain Sensitive Information.

MSJ is committed to maintaining formal practices for responding to an emergency or other occurrence that damages systems containing Sensitive Information. MSJ shall continually assess potential risks and vulnerabilities to protect Sensitive Information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures.

PROCEDURE

a. Data Backup Plan

i. MSJ, under the direction of the ISS Department Lead, shall implement a data backup plan to create and maintain retrievable exact copies of Sensitive Information.

ii. The ISS Department shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

iii. The ISS Department Lead shall direct the ISS Department to test backup procedures on an annual basis to ensure that exact copies of Sensitive Information can be retrieved and made available. Such testing shall be documented by the ISS Department. To the extent such testing indicates need for improvement in backup procedures, the ISS Department Lead and the ISS Department shall identify and implement such improvements in a timely manner.

b. Disaster Recovery and Emergency Mode Operations Plan. All MSJ disaster recovery and emergency operations plans shall be governed in accordance with existing disaster recovery plans and procedures.

References: 16 C.F.R. §314.4 (b)(3), §314.4 (c); ISO 17; NIST SP 800-53 Rev. 4 CP-2, CP-4, PM-8, PM-14.

17. SECURITY TRAINING AND AWARENESS PROGRAM

POLICY

All Workforce Members shall receive appropriate training concerning MSJ's security policies and procedures. MSJ shall also implement an awareness program to keep Users apprised of Policy requirements, as well as emerging threats. The ISS Department Lead shall keep records of all training and awareness programs and the content of the same.

PROCEDURE

a. Security Training Program ("Training Program").

i. The ISS Department Lead shall have responsibility for the development and delivery of all information security training. Such training can be accomplished through the use of software or web-based applications (such as EVERFI)

facilitated by trusted third-party vendors, in addition to in-person sessions.

ii. Security training shall be provided to all new Workforce Members as part of the orientation process when they begin work at MSJ.

iii. All Workforce Members will receive refresher training on a regularly-scheduled basis, but not less than once a year.

iv. Attendance and/or participation in such training shall be mandatory for all Workforce Members. Human Resources shall be responsible for maintaining appropriate documentation of all training activities.

b. Security Training Program Content.

i. The ISS Department Lead shall develop all training program content, including but not limited to training on applicable requirements under this Policy. Workforce Members shall be provided a copy of this Policy and any other applicable policies as part of the Security Training Program.

The ISS Department Lead shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include, at a minimum, the following:

(1) Guidance on opening suspicious e-mail attachments, e-mails from unfamiliar senders, and hoax e-mails.

(2) The importance of updating anti-virus software and or complying with any MSJ issued updates to any software.

(3) Instructions to never download files from unknown or suspicious sources.

(4) Recognizing signs of a potential virus or malware that could sneak past protective software or could arrive prior to an update to anti-virus software.

(5) The importance of saving and backing up critical data on a regular basis and storing the data in a safe place.

(6) Damage caused by viruses and worms.

(7) What to do if a virus or worm is detected.

c. Security Awareness Program.

i. The ISS Department Lead shall regularly generate and distribute to all Workforce Members security reminders. Periodic reminders should include reminders about Policy requirements, including but not limited to, topics such as password security, malicious software, incident identification and response, and access control.

ii. As part of this Security Awareness Program, the ISS Department Lead shall also generate and distribute special notices to all Workforce Members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

iii. The ISS Department Lead can provide such reminders through formal training, e-mail messages, discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, and promotional items.

iv. The ISS Department Lead shall be responsible for maintaining appropriate documentation of all periodic security reminders.

References: 16 C.F.R. §314.4 (b)(1); §314.4 (e); ISO 7.2.2; NIST SP 800-53 Rev. 4 AT-1, AT-2, AT-4, PM-13, PM-15, PM-16; NIST 800-171 3.2.1, 3.2.2, 3.2.3.

18. SECURITY MANAGEMENT PROCESS, RISK ANALYSIS AND RISK MANAGEMENT

PURPOSE

To ensure MSJ conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Sensitive Information held by MSJ.

MSJ shall conduct an accurate and thorough risk analysis to serve as the basis for MSJ's compliance efforts. MSJ shall re-assess the security risks to its Sensitive Information and evaluate the effectiveness of its security measures and safeguards at least annually, and as necessary in light of changes to business practices, technological advancements, and emerging threats.

PROCEDURE

a. The ISS Department Lead shall be responsible for coordinating MSJ's risk analysis. The ISS Department Lead shall also identify appropriate persons within MSJ to assist with the risk analysis.

b. The risk analysis shall proceed in the following manner:

i. Document MSJ's current Information Systems.

ii. Update/develop Information Systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendor, licenses, maintenance schedule, and function.

iii. Update/develop network diagram illustrating how MSJ's Information System network is configured.

iv. Update applicable physical location information.

c. For each application identified, identify each licensee (i.e., authorized user) by job title and describe the manner in which authorization is granted.

d. For each application identified:

i. Describe the data associated with that application.

ii. Determine whether the data is created by MSJ or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.

iii. Determine whether the data is maintained within MSJ only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.

iv. Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on MSJ if the application and/or related data were unavailable for a period of time.

v. Classify the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.

vi. For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.

e. Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of Sensitive Information created, received, maintained, or transmitted by MSJ. Consider the following:

i. Natural threats, e.g., earthquakes, storm damage.

ii. Environmental threats, e.g., fire and smoke damage, power outage, utility problems.

iii. Human threats.

(1) Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls.

(2) Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment.

(3) Illegal operations and intentional attacks, e.g., eavesdropping, snooping, hacking, fraud, theft, vandalism, sabotage, blackmail.

(4) External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction.

iv. Identify and document vulnerabilities in Information Systems. A vulnerability is a flaw or weakness in the ISPP, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to Sensitive Information, modification of Sensitive Information, denial of service, or repudiation (i.e., the inability to identify the source and hold some person accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities.

f. Determine and document criticality of identified risks.

i. Assign criticality level.

(1) "High" (3) is defined as having a catastrophic impact on MSJ including a significant number of MSJ records which may have been lost or compromised.

(2) "Moderate" (2) is defined as having a significant impact including a moderate number of MSJ records within MSJ which may have been lost or compromised.

(3) "Low" (1) is defined as a modest or insignificant

impact including the loss or compromise of some MSJ records.

ii. Determine risk score for each identified risk.

g. Identify and document appropriate security measures and safeguards to address key vulnerabilities.

h. Develop and document an implementation strategy for critical security measures and safeguards.

i. Determine timeline for implementation.

ii. Determine costs of such measures and safeguards and secure funding.

iii. Assign responsibility for implementing specific measures and safeguards to appropriate person(s).

iv. Make necessary adjustments based on implementation experiences.

v. Document actual completion dates.

i. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.

j. The ISS Department Lead shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The ISS Department Lead shall identify appropriate persons within MSJ to assist with such evaluations, including legal counsel. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the regulations; new federal, state, or local laws or regulations affecting the security of Sensitive Information; changes in technology, environmental processes, or business processes that may affect MSJ policies or procedures; or the occurrence of a serious security incident.

Follow-up evaluations shall include the following:

i. Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess Workforce Member compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted), and workstation sessions terminated (i.e., Workforce Members logged out); review of latest security policies and procedures for correctness and completeness;

and inspection and analysis of training, incident, and media logs for compliance.

ii. Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, MSJ shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement

References: 16 C.F.R. §314.4 (b); ISO 18.2; NIST SP 800-53 Rev. 4 CA-7, CA-8, PL-2, PM-6, PM-9, PM-12, PM-14, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5; NIST 800-171 3.4.4, 3.11.2, 3.11.3, 3.12.1, 3.12.2, 3.12.3, 3.12.4.

19. SANCTIONS POLICY

It is the policy of MSJ that all Workforce Members must protect the confidentiality, integrity, and availability of Sensitive Information at all times. MSJ will take appropriate disciplinary action against Workforce Members, contractors, or any individuals who violate MSJ's policies, state or federal law. Disciplinary action, consistent with MSJ Employee Handbook, may include termination, and referral of any matters to law enforcement when criminal activity is suspected.

References: 16 C.F.R. §314.4 (b)(1); ISO 7.2.3; NIST SP 800-53 Rev. 4 PS-8; NIST 800-171 3.3.2

20. BACKGROUND CHECKS

Where allowed under law, MSJ may conduct employment reference checks, request consumer reports or investigative consumer reports, and conduct other background investigations on any candidates for employment prior to making a final offer of employment or extension of a contract offer to independent contractors. MSJ may use a third party to conduct these background checks. MSJ will obtain written consent from individuals prior to ordering any such reports from third-party providers, and will provide a description of individual rights and all other documentation as required by law to each applicant or candidate in accordance with Fair Credit Reporting Act ("FCRA") and applicable state and federal statutes. All such reviews are subject to these notice and consent requirements.

In some cases, departments or MSJ-affiliated parties may require students and other MSJ affiliated individuals to obtain a background check before being placed in various internships, student teaching opportunities, or related responsibilities. In the event that MSJ obtains a copy of the results of the background check, the department maintaining the background check shall consider the information contained within "Sensitive Information" and apply all relevant protections.

References: 16 C.F.R. §314.4 (b)(3); NIST SP 800-53 Rev. 4 PS-3

21. DISCOVERY POLICY: PRODUCTION AND DISCLOSURE

It is MSJ's policy to produce and disclose relevant and responsive information and records in compliance with applicable laws, court procedures, and agreements made during any litigation or regulatory enforcement process. Applicable Supervisor shall contact legal counsel to coordinate and manage all such productions.

22. E-DISCOVERY POLICY: RETENTION

It is MSJ's policy to maintain and retain enterprise information and records in compliance with applicable governmental and regulatory requirements. MSJ will adhere to retention schedules and destruction procedures in compliance with regulatory, business, and legal requirements. Applicable Supervisor shall contact legal counsel to coordinate and manage all such productions.

23. INCIDENT RESPONSE PLAN AND DATA BREACH MANAGEMENT

It is MSJ's policy to develop, implement and maintain a written Incident Response Plan ("IRP") for the purposes of identifying and managing incidents in which security of Sensitive Information is put at risk. The IRP will provide MSJ personnel guidance on how to assess an incident, mitigate any harms from any incident, provide notice to appropriate parties if required by law, and to remediate any matters that lead to the incident. The IRP will also establish an Incident Response Team ("IRT") which shall have oversight and management responsibility for any incident response.

References: 16 C.F.R. §314.4 (c); ISO 16s; NIST SP 800-53 Rev. 4 IR-8.

24. RED FLAGS RULE IDENTITY THEFT PREVENTION PROGRAM

24.1 PURPOSE

The purpose of MSJ's Red Flags Rule Identity Theft Prevention Program Policy ("RFR Program") is to ensure that MSJ has reasonable policies and procedures in place that are designed to detect, prevent, and mitigate identity theft in connection with the opening of an account or any existing account as regulated by the Federal Trade Commission's Red Flags Rule Found at 16 C.F.R. Part 681. An RFR Program is required for any department or Workforce Member responsibility dealing with the processing of financial aid. Such regulated accounts are "Covered Accounts."

These policies and procedures shall be designed to accomplish the following objectives:

a. identify relevant Red Flags for the covered accounts that MSJ offers or maintains, and incorporate those Red Flags into the RFR Program;

b. detect Red Flags that have been incorporated in the RFR Program;

c. respond to any Red Flags that have been incorporated in the RFR Program;

d. ensure that the RFR Program is updated periodically to reflect changes in risks to data subjects and to the safety and soundness of MSJ from identity theft;

e. establish the framework and principles to guide the development and implementation of, and updates to, MSJ's RFR Program, and the key roles in administering and preparing the annual report on the program; and

f. track and document MSJ's identity theft prevention, detection, and mitigation activity.

Reference: 16 C.F.R. § 681.1(a)-(d).

24.2 SCOPE

This Policy applies to all of MSJ's administrative, technical, and physical policies, procedures, and practices concerning the opening and maintenance of Covered Accounts that relate to the prevention, detection, and mitigation of identity theft. The development, implementation, maintenance, and execution of the Identity Theft Prevention Program are the joint responsibility of Workforce Members that handle Sensitive Information in their performance of work for MSJ. Workforce Members are expected to cooperate fully with any assessment of Red Flags conducted as part of the RFR Program in departments for which they are accountable.

Reference: 16 C.F.R. § 681.1(a)-(d)

24.3 GUIDELINES FOR IDENTIFYING RED FLAGS

In designing and updating the RFR Program, MSJ shall consider the following:

a. the types of Covered Accounts offered or maintained by MSJ;

b. the methods used to open Covered Accounts;

c. the methods provided to access Covered Accounts; and

d. MSJ's previous experiences with identity theft.

Further, when incorporating Red Flags into the RFR Program, MSJ shall consider the following:

e. identity theft incidents MSJ has incurred or identified as a potential risk;

f. applicable Supervisory guidance, notifications, alerts, or warnings issued by the FTC, the national credit reporting agencies (Equifax, TransUnion, Experian), law enforcement, or other reliable sources of information relating to identity theft risk;

g. the presentation of suspicious documents;

h. login entries from unknown or unauthorized devices;

i. the presentation of suspicious personally identifiable information;

j. the usual use of, or other suspicious activity related to a Covered Account; and

k. notice from data subjects, victims of identity theft, law enforcement authorities, consumer reporting agencies, or other persons regarding identity theft in connection with Covered Accounts.

All identified Red Flags relevant to MSJ shall be documented by the ISS Department Lead or other authorized personnel.

Reference: 16 C.F.R. § 681.1(c)-(d)

24.4 GUIDELINES FOR DETECTING RED FLAGS

The policies, procedures, and practices of the RFR Program must address the relevant Red Flags that MSJ may detect in connection with opening Covered Accounts or activity related to existing Covered Accounts. These shall include, but are not limited to:

a. Obtaining personally identifiable information about, and verifying the identity of, a person opening a Covered Account;

b. authenticating data subjects, monitoring transactions, and verifying the validity of change of address requests for existing Covered Accounts;

c. locking a Covered Account after three (3) failed login attempts; and

d. providing data subjects with the option for multi-factor authentication login.

Reference: 16 C.F.R. § 681.1(c)-(d)

24.5 GUIDELINES FOR PREVENTING AND MITIGATING IDENTITY THEFT

The policies, procedures, and practices of the RFR Program should provide responses to the detected Red Flags that are appropriate when balanced against the degree of risk posed. In determining an appropriate response, MSJ shall give consideration to any aggravating factors that may increase the risk of

identity theft, such as a data breach or phishing occurrence. Workforce Members shall also adhere to the requirements in Section 2.5 ("Reporting Software or Hardware Malfunctions") and Section 2.6 ("Report Security Incidents") as such incidents may constitute Red Flags.

Reference: 16 C.F.R. § 681.1(c)-(d)

24.6 DOCUMENTATION OF DETECTED RED FLAGS

Any identified Red Flags should be documented in writing in the Network Access Form, and in any written policies or procedures, as needed.

Reference: 16 C.F.R. § 681.1(c)-(d)

24.7 SERVICE PROVIDER ARRANGEMENTS

When MSJ engages a Service Provider to perform an activity in connection with Covered Accounts, MSJ must take steps to confirm that the Service Provider's activity is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. MSJ shall negotiate written contracts with Service Providers that require the Service Provider to:

a. have policies in place to detect relevant Red Flags (such as credit monitoring alerts, logins from unknown devices, etc.) that may arise in the performance of the Service Provider's activities using, at a minimum, the same standards that MSJ would take if performing the tasks itself; and

b. either report any identified Red Flags to MSJ, or take appropriate steps to prevent or mitigate identity theft. Such steps should be documented and summarized to MSJ.

The ISS Department Lead shall be responsible for identifying all applicable Service Provider arrangements and confirming that they meet these requirements.

Reference: 16 C.F.R. § 681.1(c)-(d)

24.8 UPDATING THE RFR PROGRAM

MSJ shall annually determine whether the RFR Program requires modification. As part of this determination, MSJ shall consider changes in the following activities or processes:

a. methods that MSJ uses to open or access Covered Accounts;

b. MSJ's previous experiences with identity theft;

c. MSJ's methods to detect, prevent, and mitigate identity theft; and

d. MSJ's business arrangements, including mergers, acquisitions, alliances, joint ventures, and Service Provider agreements.

Any changes to the RFR Program, and the reasons for making such changes, should be documented in the Network Access Form.

Reference: 16 C.F.R. § 681.1(d)-(e)

24.9 ADMINISTRATION OF RFR PROGRAM

ISS Department Lead shall be responsible for oversight, development, implementation, and administration of the RFR Program.

Oversight obligations include, but are not limited to:

a. assigning specific responsibility for the RFR Program's implementation;

b. reviewing reports prepared by authorized personnel regarding compliance with the RFR Program requirements;

c. approving material changes to the RFR Program as necessary to address changing identity theft risks; and

d. confirming there is appropriate and effective oversight of Service Provider arrangements.

In addition, MSJ shall train its Workforce Members, as necessary, to effectively implement the RFR Program.

Reference: 16 C.F.R. § 681.1(e)

24.10 ANNUAL COMPLIANCE REPORT

The ISS Department Lead, in coordination with authorized personnel responsible for the development, implementation, and administration of the RFR Program, shall compile an annual report on MSJ's compliance with the RFR Program requirements. At a minimum, the annual report shall address the following:

a. the effectiveness of MSJ's policies and procedures in addressing the risk of identity theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts;

b. Service Provider arrangements;

c. significant incidents and data breaches involving identity theft from the past year and MSJ's response to such incidents; and

d. recommendations for any material changes to the RFR Program.

Reference: 16 C.F.R. § 681.1(e)

Mount St. Joseph University	Records Retention Schedule				
Department/Function	**Document**	**Retention Period**	**Notes**	**Applicable Law**	**Notes/Explanation**
General/Corporate					
	Annual or Summary Reports	Permanent		Ohio Rev. Code Ann. § 1713.03	
	Attorney Opinion Letters (Real Estate)	Permanent			
	Final College Budget	Permanent	Maintained in Archives		
	Contracts and Agreements	10 years after Termination		Ohio Rev. Code Ann. § 2305.06.; Ohio Rev. Code Ann. § 2305.14.	
	Correspondence - Legal	Permanent			
	Correspondence - Regulatory	Permanent			
	Deeds and Titles	Permanent			
	Deeds and Titles for Donated Real Property Later Sold	21 years			
	General / Routine Correspondence	Indefinite	Destroy when no longer useful		
	Strategic Planning Documents	Indefinite	Destroy when no longer useful		
	Mortgage, Bond and Long-term Debt Records	Permanent			
	Bond Documents	Permanent			
	Property Records	Active+5 years			
	Sales of Property Records	21 years			
	Special Correspondence	Indefinite	Destroy when no longer useful		
	Formal Speeches and Papers Presented by President	Permanent			
	HLC Accreditation reviews and reports & Self Study Documents	Permanent			

	Federal Financial Responsibility	Permanent		34 CFR § 664.24	
	College Committee Assignments	Indefinite	Destroy when no longer useful		
	State of Ohio Certificate and Charter number records	Permanent			
	Other state certificates of authority	Permanent	State of Kentucky		
	College Committee Meeting Minutes	Indefinite	Destroy when no longer useful		
Board of Trustees					
	Articles of Incorporation	Permanent		Ohio Rev. Code Ann. § 1701.37	
	Board of Trustees Meeting Minutes	Permanent		Ohio Rev. Code Ann. § 1701.37	
	By-laws	Permanent		Ohio Rev. Code Ann. § 1701.37	
	Board Committee Meeting Minutes	Permanent		Ohio Rev. Code Ann. § 1701.37	
	Minutes of Board Standing/Ad Hoc/Special Appointed Committees	Permanent	Separate documents or reflected in board committee minutes	Ohio Rev. Code Ann. § 1701.37	
Academic Administration					
	Faculty Name & Address Lists	Indefinite	Destroy when no longer useful		
	Informational and Reference Material	Indefinite	Destroy when no longer useful		
	Minutes of Administrative/Faculty/Department Meetings	Indefinite	Destroy when no longer useful		
	Periodic Reports	Indefinite	Destroy when no longer useful		

	Professional Development and Sabatical Request	Personnel File (Termination Date + 7 years).	Destroy Duplicates after combining files		
	Promotion & Tenure Committee Actions	Permanent		29 C.F.R. § 1602.49	
	Faculty Evaluations	Termination Date + 7 years			
	Faculty Course Evaluations	Personnel File (Termination Date + 7 years).			
	Faculty Contracts for Course Development & Intellectual Property Rights	Indefinite	Destroy when no longer useful	Ohio Rev. Code Ann. § 2305.06.; Ohio Rev. Code Ann. § 2305.14.	
	Grade Appeal Support	5 years after appeal			
	Full time and adjunct faculty contracts	10 years		Ohio Rev. Code Ann. § 2305.06.; Ohio Rev. Code Ann. § 2305.14.	
	High School Dual Enrollment Student Enrollment Form (copies)	last date of attendance + 5 years	Originals forwarded to SAS		
ISS					
	Email Backup	1 year			
	Employee Directories	5 years			

	Software licenses and support agreements	10 years after all obligations end		Ohio Rev. Code Ann. § 2305.06.; Ohio Rev. Code Ann. § 2305.14.	
	Trademarks, registration, patents, and copyri	Permanent			
	CX backups	Indefinite	Destroy when no longer useful		
	Course materials stored in Learning Management System	7 years			
	College archives	Indefinite			
Institutional Research					
	IPEDS	Permanent	Archive after 6 years		
	Other External Surveys	Indefinite	Destroy when no longer useful		
	Internal Statistical official records	Indefinite	Destroy when no longer useful		
	Graduate and Transfers Rate calculation	Permanent	Archive after 6 years	34 C.F.R. § 668.45	
	Degree Statistics	Permanent	Archive after 6 years		
	Enrollment Statistics	Permanent	Archive after 6 years	ORC 3365.15; OAC 3333-1-02; OAC 3333-1-65.5	
	Race/ethnicity statistics	Permanent	Archive after 6 years		
Student Financial Services					
	FSA Program Participation Agreement	Permanent		34 CFR §668.14	
	FISAP	End of year report submitted +3 years		34 C.F.R. §668.24(1)	
	Pell Grant SOA	Indefinite until Superceded		34 C.F.R. §668.24(1); 34 C.F.R. §674.19	

	FSA Program Reconciliation reports	Keep with other FSA documents (i.e. end of year of report +3 years)		34 C.F.R. §668.24	
	Other FSA admin. Documents	End of year report submitted +3 years		34 C.F.R. §668.24	
	FSA/Campus Based (Pell, ACG/SMART)	End of aid award year + 3 years		34 C.F.R. §668.24	
	Perkins/NSL repayment records	Loan cancel date or paid date or assigned date +3 years		34 C.F.R. §674.19; 34 C.F.R. §668.24	
	Perkins/NSL Promissory notes	3 years after loan satisfaction		34 C.F.R. §674.19; 34 C.F.R. §668.24	Must retain for three years from cancellation, repayment or other satisfaction. If original note is retained (i.e. when not signed electronically), must be kept in fire-proof container.
	FFEL and Direct Loans	End of award year student last attended + 3 years		34 C.F.R. §668.24	

	All other DOE records	End of year report submitted +3 years		34 C.F.R. §668.24	
Insurance /Risk Management					
	Accident reports	7 years			No legal authority found but Insurance policies may have retention requirements to consider.
	Claims (after settlement)	7 years			No legal authority found but Insurance policies may have retention requirements to consider.
	Fire/property inspection records	7 years		29 C.F.R. § 1910.157	The cited regulation requires an employer to retain records annual maintenance for fire extinguishers for 1 year . However, insurance policies may have longer retention requirements to consider.
	Records and policies	Active + 7 years			
	Court Documents and Records	Active +2 years with litigation files			

	Deposition Transcripts	Active +2 years with litigation files			
	Discovery Materials	Active +2 years with litigation files			
	Litigation Files	Active+2 years			These documents should be kept together with court documents/records, deposition transcripts, and discovery materials
	Property Insurance Records	Active + 7 Years			
	Liability Insurance Policies	Active + 7 Years			
	Insurance Claim Documents	Active + 7 Years			
Compliance					
	Grievances or reported violations of: Title IX, VI, VII, Rehabilitation Act	7 years after resolution		29 C.F.R. §1602.14	
Tax					
	Correspondence - accountants	7 years after applicable return is filed			
	IRS exemption determination and related correspondence	Permanent			
	IRS Form 990s	Permanent			
	Property Tax Exemption Records	Permanent			

	Sales, use and property tax returns/records	7 years		26 C.F.R. § 301.6501(a)-1; 26 C.F.R. § 301.6501(e)–1; 26 U.S.C. 6531;	The general IRS statute of limitation is 3 years. 26 C.F.R. § 301.6501(a)-1. However, the limitations period is 6 years when an organization omits substantial income from its return (i.e. over 25% of the income stated on the return). 26 C.F.R. § 301.6501(e)–1. Therefore, it is logical/prudent to retain tax records for 7 years. The statute of limitations for criminal actions is also 6 years. 26 U.S.C.A. § 6531. .
Career Center/Co-Op					
	Student Employment Agreements	7 years		29 C.F.R. §516.30	
	Student Job Descriptions	7 years			
	Other documents	7 years			
Financial Records					

	1099's	7 years			No legal authority found for retention of routine financial records. However, it is logical/prudent to retain these records in consideration of IRS statutes of limitation. Hence, it is logical/prudent to retain these records for 7 years. The general IRS statute of limitation is 3 years. 26 C.F.R. § 301.6501(a)-1. However, the limitations period is 6 years when an organization omits substantial income from its return (i.e. over 25% of the income stated on the return). 26 C.F.R. § 301.6501(e)–1. The statute of limitations for criminal actions is also 6 years. 26 U.S.C.A. § 6531.
	Account Reconciliations	7 years			See above notes for 1099's
	Accounts Receivable Collection Records	Current+7 years			See above notes for 1099's
	Accounts Receivable Detail	7 years			See above notes for 1099's
	Annuity Documentation	Permanent			
	Audit Reports and Workpapers (Financial & Compliance)	7 years			See above notes for 1099's
	Audited Financial Statements/Auditor Management Letters	Permanent-Archived			

	Bank Reconciliations/Statements	7 years from date filed			See above notes for 1099's
	Budget Workpapers	Indefinite	Destroy when no longer useful		See above notes for 1099's
	Budget Summary	Permanent			See above notes for 1099's
	Cost Center Detail	7 years			See above notes for 1099's
	Cash Receipts	7 years			See above notes for 1099's
	A/P documents/Credit Card Records/Expense Reports	7 years			See above notes for 1099's
	Fixed Asset Detail (Invoices, etc)	7 years			See above notes for 1099's
	Fixed Asset Summary Records	Permanent			
	General Ledgers and Operating Ledgers	Permanent			
	Investment Detail Records	7 years			See above notes for 1099's
	Investment Summaries	Permanent			
	Inventory Records	7 years			See above notes for 1099's
	Life Income Agreements	Permanent			See above notes for 1099's
	Loan Documentation	Permanent			
	Subsidiary Ledgers	7 years			See above notes for 1099's
	Swap Documentation	Permanent			See above notes for 1099's
	Wire Transfer Records	7 years			See above notes for 1099's
	Unclaimed Property Records	7 years			See above notes for 1099's
	Federal Cash Transactions	7 years			See above notes for 1099's

Grants- Federal/State/Private					
	Federal Grants	Permanent		34 C.F.R. § 668.24 (1) ; 2 C.F.R. § 200.333	
	Government Filings	Permanent			
	Private Grants	Permanent			
	State Grants	Permanent	Must store in a fireproof safe		
Registrar					
	Course Catalogs	Permanent			
	Name Change Authorization	7 years	Provide immediately to Fiscal for Red Flag		
	Student File:				
	Transcript Records/HS information from admission process	Permanent			
	Transfer information				
	Class lists	Permanent			
	Commencement Program	Permanent	Archive after 6 years		

	FERPA related challenges/documentation/training	Permanent			24 CFR § 99.32 requries maintaining a record of each request for access to and each disclosure of personally identifiable information from the education records of each student as long as the records are maintained. 34 CFR § 99.10(e) prohibits the destruction of education records if there is an outstanding request to inspect and review the records.
	VA Certifications	last date of attendance + 5 years			
Admission					
	Student Application without registration	3 years			
	Student Advising File once admitted	last date of attendance + 5 years			
	Student VISA Information	Indefinite		8 C.F.R. § 214.3(g)	Required to retain for three years after the student is no longer pursuing a full course of study.
Human Resources					

	Bureau of Workers Compensation premium and claim(s) information/documentation	10 years		Ohio Rev. Code Ann. § 4123.52; Ohio Admin. Code 4123-17-17	Ohio Rev. Code Ann. § 4123.52 gives the industrial commission of the Ohio Department of Workers' Compensation continuing jurisdiction over workers' comp cases for 5 years from the date of the injury. Therefore, these records should be retained for at least five years, however it may be wise to retain longer.
	Employee handbooks (one set)	Permanent			
	Employee personnel records (offer letters, performance evaluations, discipline, commendations, employee statements, investigation notes	7 years after termination from employment	Maintain scan of necessary documentation for 403b audit	29 C.F.R. § 1602.14	
	Form I-9 (stored separate from personnel file)	Termination of employment + 1 year or hire date + 3 years for earlier termination		8 CFR §274a(2)(b)(2)	Required to keep three years after the date of the hire or one year after the date the individual's employment is terminated, whichever is later

	OSHA forms related to injuries and illness	End of reported year + 5 years		29 C.F.R. § 1904.33	"(a) Basic requirement. You must save the OSHA 300 Log, the privacy case list (if one exists), the annual summary, and the OSHA 301 Incident Report forms for five (5) years following the end of the calendar year that these records cover."
	OSHA records related to medical exams or records indicating exposure to toxic substances	30 years after termination from employment		29 C.F.R. §1910.1020	
	Payroll records (compensation history, pay rate, payroll deductions, time cards)	3 years after termination from employment		29 C.F.R. § 516.5; 29 C.F.R. § 516.6;Ohio Rev. Code Ann. § 4111.08; 29 C.F.R. § 1627.3	Required to keep for three years.
	Retirement plan benefits (plan descriptions, plan documents)	Permanent		29 U.S.C. § 1027; 29 C.F.R. § 2520.107-1	Required to keep for six years.
	Non-retirement benefit plan records (plan descriptions, plan documents, contracts, summary annual reports, 5500s, etc)	6 years		29 U.S.C. § 1027; 29 C.F.R. § 2520.107-1	Required to keep for six years.

	Solicited employment applications/resumes of non-employees	1 year from date of hiring decision or until resolution of any pending charge or action by EEOC or Attorney General.		29 C.F.R.§ 1602.14; 29 C.F.R. § 1627.3(b)	Per, 29 CFR § 14, "Where a charge of discrimination has been filed, or an action brought by the Commission or the Attorney General, against an employer under title VII, the ADA, or GINA, the respondent employer shall preserve all personnel records relevant to the charge or action until final disposition of the charge or the action."

	Unemployment compensation documentation	7 years		26 C.F.R. § 31.6001-1; 26 C.F.R. § 301.6501(a)-1; 26 U.S.C. 6531;	The IRS requires employment related tax records be kept for 4 years. 26 C.F.R. § 31.6001-1. However general IRS statutes of limitation should also be considered. The general IRS statute of limitation is 3 years. 26 C.F.R. § 301.6501(a)-1. However, the limitations period is 6 years when an organization omits substantial income from its return (i.e. over 25% of the income stated on the return). 26 C.F.R. § 301.6501(e)–1. Therefore, it is logical/prudent to retain tax records for 7 years. The statute of limitations for criminal actions is also 6 years. 26 U.S.C.A. § 6531.
	FMLA Records and Notices	3 years		29 C.F.R. § 825.500; 29 C.F.R. Part 516	Required to keep for 3 years.

	Records related to higher Education Staff Information Report EEO-6	3 years		29 C.F.R. § 1602.48- 29 C.F.R. § 1602.50	EEO-6, Higher Education Institution Staff Information Report. Under 29 C.F.R. § 1602.48, this document, and the information needed to create it is required to be retained for three years.
Payroll					
	Forms 941 and 945	7 years		26 C.F.R. § 31.6001-1; 26 C.F.R. § 301.6501(a)-1; 26 U.S.C. 6531;	The IRS requires employment related tax records be kept for 4 years. 26 C.F.R. § 31.6001-1. However general IRS statutes of limitation should also be considered. The general IRS statute of limitation is 3 years. 26 C.F.R. § 301.6501(a)-1. However, the limitations period is 6 years when an organization omits substantial income from its return (i.e. over 25% of the income stated on the return). 26 C.F.R. § 301.6501(e)–1. Therefore, it is logical/prudent to retain tax records for 7 years. The statute of limitations for criminal actions is also 6 years. 26 U.S.C.A. § 6531.

	Garnishments	Active		29 C.F.R. §516.6(c) (1)	Required to keep at least 2 years.
	Notices of Employment Security Claims	2 years			
	Payroll Deductions	3 years		29 C.F.R. §516.6(c) (1)	Required to keep at least 2 years.
	Payroll Master Control/Register	3 years		29 C.F.R. §516.5	Required to keep at least 3 years.
	Payroll Records - Other	3 years		29 C.F.R. §516.5	Keep at least 3 years.
	Salary or Current Rate of Pay	3 years		29 C.F.R. §516.5	Required to keep at least 3 years.
	Student Timesheets	3 years		29 C.F.R. §516.30; 29 C.F.R. §519.17	Required to keep at least 3 years.
	Timesheets	2 years from last entry		29 C.F.R. §516.6(c) (1)	Required to keep at least 2 years from last entry.

	W-2 and W-4 Forms	7 years		26 C.F.R. § 31.6001-1; 26 C.F.R. § 301.6501(a)-1; 26 C.F.R. § 301.6502–1; 26 U.S.C. 6531;	The IRS requires employment related tax records be kept for 4 years. 26 C.F.R. § 31.6001-1. However general IRS statutes of limitation should also be considered. The general IRS statute of limitation is 3 years. 26 C.F.R. § 301.6501(a)-1. However, the limitations period is 6 years when an organization omits substantial income from its return (i.e. over 25% of the income stated on the return). 26 C.F.R. § 301.6501(e)–1. Therefore, it is logical/prudent to retain tax records for 7 years. The statute of limitations for criminal actions is also 6 years. 26 U.S.C.A. § 6531.
	Wage or Salary History	3 years		29 C.F.R. §516.5	Required to keep at least 3 years.
	Wage Rate Tables	7 years		29 C.F.R. §516.6(a)(2)	

Plant					
	Building Permits	Active+5 Years			
	Building Plans and Specifications	Permanent			
	Maintenance Records	Active			
	Office Layouts	Active			
	Operating Permits	Active			
	Property Improvement Records	Active+5 Years			
	Zoning Permits	Active			
Environmental Health & Safety					
	Air or Water Waste Emissions	3 years			
	Hazardous Chemical Waste Records	5 years		40 C.F.R. § 262.11	
	Laboratory Practices	Active			
Development					
	Private Grant Files - unfunded	1 year			
	Private Grant Files - funded	7 years after closure			
	Gift Records	Current + 7 years			
	Endowed Gifts records	Permanent			
Athletics					
	Certification of Compliance	6 years			
	Certification of Eligibility	6 years			
	Certification for Particular Sport	6 years			
	Eligibility Certification by Sport, per Semester	6 years			
	Sports Sponsorship and Demographics	6 years			
	Equity in Athletics Disclosure Report	6 years		34 C.F.R.§ 668.47	

	NCAA Annual Report of Revenues and Expenditures	6 years			
	Notification of Completion of Institutional Self-Study (completed once every 5 years)	6 years			
Public Safety					
	Campus Crime Reports - Annual	4 years		20 U.S.C. §1092 and 34 C.F.R. Part 668	
	Campus Crime Reports - Interim	2 years			
	Motor Vehicle Records	Active			
	Parking Violations / Tickets	3 years			
Residence Life					
	Housing Records	7 years/Permanent			
Student Affairs					
	Disciplinary Records	7 years from last date enrolled or resolution			
Student Disability Services					
	Project EXCEL Student Disability Services File	Active + 7 years			
	Disability Services Student File	Active + 7 years			
	Learning Center Tutor Request Forms	1 year			
Wellness					
	Counseling Records	7 years from last session date			

	Health Services: Immunizations given on campus	Permanent			
	Health Services: Medical Records	7 years from last date enrolled or graduated			
	Influenza immunizations	1 year			
	Alcohol/Drug Biennial Reviews	3 years		34 C.F.R. § 86.103(b)	The university's drug prevention program certification should also be maintained.

Rev 2022

72868702v2