XAVIER UNIVERSITY

Information Security Policy

Effective: 2/22/2018

Last Updated: 3/08/2018

Responsible University Office: Information Security Office

Responsible Executive: Associate Provost and Chief Information Officer

Scope: This policy applies to all University owned information that is present on or transmitted through University owned systems and networks. University owned information assets can take the form of electronic and hard copy information.

A. REASON FOR POLICY

This document defines the Information Security Risk Management Program (Risk Management Program) for Xavier University. Xavier University is committed to protecting the confidentiality, integrity and availability of information assets from all threats including unauthorized access, modification or damage while also providing for the open information sharing requirements of academic freedom. The purpose is to establish the University's approach to information security risk management and define the appropriate controls that are required to prevent compromises to information assets. The purpose of this Risk Management Program is to describe the policy and practices that identify information security threats, assess the vulnerability of Xavier information systems to those threats, and reduce risk to Xavier data and systems in compliance with applicable laws and standards. The objective of Xavier's Risk Management Program is to support Xavier's mission while also mitigating financial, operational, reputational and regulatory compliance risk. This Risk Management Program shall enable Xavier to accomplish its mission(s) by:

1. Securing the Information Systems that create, maintain, process, or transmit Xavier data.
2. Enabling the appropriate Xavier personnel to make well- informed decisions regarding risk and risk management.
3. Collaborating with other Xavier risk management activities to ensure Xavier priorities are aligned.

Ownership, Review and approval

The Associate Provost and Chief Information Officer owns this policy. The Information Security Policy is approved as defined by the Policy Development Process at Xavier University. It is reviewed on an annual basis for update or when significant change is required by the Information Security Office.

Audience

The Terms apply to all individuals that have access to Xavier's information resources, including but not limited to: all faculty, staff, students, alumni, retirees, temporary workers, library patrons, visitors, contractors and vendors using University information resources, whether on- or off-site (hereafter collectively referred to as "Users").

B. POLICY

The Xavier Information Security Office will perform risk assessments on all proposed hardware and software acquisitions, and data transmissions and periodic risk assessments of installed software applications and hardware configurations. This is to ensure that Xavier's risk posture is maintained at the lowest exposure attainable.

C. DEFINITION

For the purposes of this document, these words and phrases have the following meanings:

Asset – Any Information System that is a part of Xavier's business processes

Information System – A workstation, server, or other information technology resource owned and/or managed by Xavier used for electronic storage, processing or transmitting of any data or information

Intellectual Property – Intellectual Property is any intangible asset that consists of human knowledge and ideas. Some examples are patents, copyrights, trademarks and software.

Risk – Risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. Risk is usually calculated as either a quantitative or qualitative score, and can be represented in the following equation:

Risk = (Likelihood of Threat/Vulnerability Event Occurrence) X (Business Impact of Event Occurring)

- **Inherent Risk –** Inherent Risk is defined as the likelihood and impact of loss arising out of circumstances or existing in an environment or Information System, in the absence of any action to control or modify the circumstances.

- **Residual Risk –** Residual Risk is the risk of an Information System that remains after controls or other mitigating factors have been implemented.

Threat – A threat is anything (natural, facility, and/or human) that has the potential to cause harm.

User – Any person, including full-time employees, faculty, students, alumni, retirees, part-time employees, temporary employees, contractors, vendors and affiliates, who accesses Xavier's Information systems.

Vulnerability – A vulnerability is a weakness that could be used to endanger or cause harm to an Asset.

Workstation – An electronic computing device, (for example a laptop, tablet, smartphone, or desktop computer) or any other device that performs similar functions

D: PROCEDURES

Methodology:

Risk Management Program is formed primarily on the NIST Special Publication 800-30 "Risk Management Guide for Information systems" methodology. The Information Security Control Framework is based foremost on the NIST 800-53 rev 5 and ISO27002 control frameworks. Xavier will incorporate any additional controls required by regulatory compliance and contractual obligations as they arise.

The Risk Management Program consists of following three phases.

- Phase 1 - Risk Analysis
- Phase 2 - Risk Assessment
- Phase 3 - Risk Management

Phase 1 – Risk Analysis

The Risk Analysis process will take into account a Threat Assessment conducted on the university campus, the assignment of a Risk Probability, and the determination of the Risk Impact.

A. <u>Threat Assessment</u>

Xavier shall conduct a probabilistic risk analysis of threats and vulnerabilities that may impact its campus. This risk analysis includes the following threat types:

- Natural threats, such as hurricane, earthquake, etc
- Facility threats, such as electrical failure, HVAC failure, etc
- Human threats, such as malware, employee error, etc

1. <u>Risk Probability</u> - The probability, or likelihood, that a natural or facility threat will occur, or that a human threat agent will exploit vulnerabilities will be scored on a scale of 1-5, with the likelihood considerations rated as follows:

Likelihood Level	Quantitative Value	Likelihood Definition Anticipated frequency of occurrence (based on an average over the past 10 years) is:
Very High	5	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	4	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
Medium	3	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
Low	2	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Negligible	1	Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

Adapted from NIST 800-30 Appendix G

2. Risk Impact - The exercise of natural, facility, and human threats exploiting vulnerabilities will be analyzed against their impact on the following factors:

- Confidentiality- Ensuring that authorized personnel have access to information and facilities they need, and that unauthorized personnel do not gain access
- Integrity - Providing accurate, timely and complete information that meets the requirements of management, staff, customers, suppliers and regulators
- Availability - Keeping existing systems running and recovering from interruptions

Each of these factors will be scored on a scale 1-5, with the impact considerations rated as follows:

Magnitude of Impact	Quantitative Value	Impact Definition
Very High	5	The threat event could be expected to have multiple severe or catastrophic adverse effects on confidentiality, integrity, and availability.
High	4	The threat event could be expected to have a severe or catastrophic adverse effect on confidentiality, integrity, and availability. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of business mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Medium	3	The threat event could be expected to have a serious adverse effect on confidentiality, integrity, and availability. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in business mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	2	The threat event could be expected to have a limited adverse effect on confidentiality, integrity, and availability. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in business mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Negligible	1	No significant impact. The threat event could be expected to have a negligible adverse effect on confidentiality, integrity, or availability.

Adapted from NIST 800-30 Appendix H

PHASE 2 – Risk Assessment
The Risk Assessment is conducted by determination of the Inherent Risk, review of security Controls Effectiveness, and the determination of Residual Risk.

A. Determining Inherent Risk

Inherent Risk scores are calculated based on the following five (5) vectors of risk:

1. The highest classification of data stored on an Information System.
2. The platform used to access an Information System.
3. The types of users who access an Information System.
4. The number of users who access an Information System.
5. The number of individual data records stored on an Information System.

B. Determining Control Effectiveness

Control effectiveness is calculated based on evaluation of the results of the controls implemented *and* based on the evaluation of a failure in the "Mandatory Control" list. The following details the method for designating control effectiveness for each rating:

Control Effectiveness Rating	Percentage of Compliance
HIGHLY EFFECTIVE	> 90%
EFFECTIVE	> 80%
PARTIALLY EFFECTIVE	> 70%
INEFFECTIVE	< 70% ***-OR-*** Information System fails on any one of the Mandatory Controls*

Adapted from NIST 800-30 Appendix I

1. Control Implementation
   Control implementation will be assessed using a six-tier system based on the Carnegie Mellon Capability Maturity Model. Controls that do not meet at minimum the repeatable maturity level will be considered a failed implementation.
2. The maturity levels are as follows:
   a. Nonexistent
      There is no evidence of this standard or practice in the organization.
   b. Initial
      The organization has an ad hoc and inconsistent approach to this standard or practice.

c. Repeatable
   The organization has a consistent overall approach, but it is mostly undocumented.
d. Defined
   The organization has a documented detailed approach, but no routine measurement.
e. Managed
   The organization regularly measures its compliance and makes regular process improvements.
f. Optimized
   The organization has refined its compliance to the level of best practice.

* Mandatory Controls – Mandatory Controls are controls that Xavier requires to be implemented as stated for all Information systems, regardless of Inherent Risk score. Mitigating controls or any exceptions to policy may not be considered to reduce the Residual Risk of the Information System if any of the following controls fail:

Control Number	Control Question
11.2.1.1.H	Are the Users of this information system uniquely identified?
11.2.1.2.H	Is this information system configured to restrict User privileges to only those needed to perform authorized tasks related to an assigned job role?
11.2.3.1.H	Are the users of this information system authenticated (with password, PIN, or other token) before receiving access to information and functionality?

Adapted from NIST 800-30 Appendix I

C. Determining Residual Risk

Residual Risk is determined based on the combination of two elements: Inherent Risk rating and control effectiveness rating. The following table shows the resulting Residual Risk score:

		Inherent Risk Score		
		LOW	MEDIUM	HIGH
Control Effectiveness	HIGHLY EFFECTIVE	**LOW**	**LOW**	**MEDIUM-LOW**
	EFFECTIVE	**LOW**	**MEDIUM-LOW**	**MEDIUM**
	PARTIALLY EFFECTIVE	**LOW**	**MEDIUM-LOW**	**MEDIUM-HIGH**
	INEFFECTIVE	**LOW**	**MEDIUM**	**HIGH**
		Residual Risk Score →		

Adapted from NIST 800-30 Appendix I

PHASE 3 – Risk Management

The Director of Information Security shall issue both Inherent and Residual Risk scores in risk assessment summary reports for all Information systems assessed. The Director of Information Security will also establish priorities and timelines for future assessments and verify ongoing compliance with applicable laws and standards. The Chief Information Officer will make the final determination on remaining Residual Risk that cannot be remediated to a low overall risk score either accepting the risk as scored or requiring further vendor remediation.

Exceptions to Policy and Risk Acknowledgement

Information Systems provide protection for Xavier assets that are often required by best practice, regulations or contractual obligations. Failing to comply with a control and granting an exception should be only due to unreasonable compliance expense or effort and should be temporary. The exception to policy and risk awareness process applies to instances where the cost to remediate systems and processes which are not compliant with applicable policies, standards, and procedures greatly exceeds the risks of non-compliance. The Chief Information Officer may grant this exception.

All approved exceptions to policy will have an expiration date and will be reviewed prior to expiration. This ensures that Xavier's assumptions or business conditions have not changed. The Associate Provost and Chief Information Officer will reapprove the request if the exception to policy is still valid.

Risk Management Program Review

The Risk Management Program shall be reviewed annually.

Responsibilities

The following defines the information security roles and responsibilities at Xavier.

Associate Provost and Chief Information Officer:

The Chief Information Officer provides Executive oversight to the risk management process in accordance with applicable laws and standards to help the organization secure Xavier data and information systems. The Chief Information Officer reserves the right to override the Residual Risk scores of Xavier Information systems as necessary to accurately reflect the risk an information system poses to Xavier. The Chief Information Officer will make the final determination on remaining Residual Risk that cannot be remediated to a low overall risk score either acknowledging the risk as scored or allocating appropriate time, money and/or other resources to remediate control failures and reduce the Residual Risk to an acceptable level for Xavier. The Chief Information Officer will have final approval or denial of appeals of negative decisions on any exception to policy.

Director of Infrastructure:

The Director of Infrastructure as directed by the Chief Information Officer provides oversight to the risk management process in accordance with applicable laws and standards to help the organization secure Xavier data and Information systems. The Director of Infrastructure reserves the right to override the Residual Risk scores of Xavier information systems to a higher level as necessary to accurately reflect the risk an Information System poses to Xavier.

Executive Director Application Services & Technology Service Center:

The Executive Director Application Services & Technology Service Center as directed by the Chief Information Officer provides oversight to the risk management process in accordance with applicable laws and standards to help the organization secure Xavier data and Information systems. The Executive Director reserves the right to override the Residual Risk scores of Xavier information systems to a higher level as necessary to accurately reflect the risk an Information System poses to Xavier.

Director of Web services

The director of web services as directed by the Associate Vice President, Marketing & Communications provides oversight to the risk management process in accordance with applicable laws and standards to help the organization secure Xavier data and web-based Information systems. The Director reserves the right to override the Residual Risk scores of Xavier web information systems to a higher level as necessary to accurately reflect the risk a Web based Information System poses to Xavier.

Associate Vice President, Enrollment Management and Student Success
The Associate Vice President, Enrollment Management and Student Success provides oversight to the risk management process in accordance with applicable laws and standards to help the organization secure Xavier data and enrollment management information systems. The Associate Vice President reserves the right to override the Residual Risk scores of Xavier enrollment management information systems to a higher level as necessary to accurately reflect the risk an enrollment Information System poses to Xavier.

Information Owner: The Information Owner is the President's Direct Report or their designee that is responsible for overseeing the security of their division's information. Responsibilities include:

- Authorize access to departmental information based on need to know.
- Oversee the proper handling of information.
- Define information assets that are sensitive in nature.
- Assist users in applying the appropriate security controls to information assets.
- Recertify user access to information on a periodic basis.
- Understand information use and the associated risks including improper disclosure.
- Work with Information Technologies to define controls to protect the confidentiality, integrity and availability of information assets.
- Ensure that the department operates in compliance with the Information Security Policy.
- Ensure that information assets are protected in a manner that is commensurate with regulatory mandates.

Information Security Office: The Information Security office responsibilities under the direction of the Director of Information Security include:

- Oversee Information Security initiatives at the University.
- Stay abreast of current threats and information security best practices.
- Perform vulnerability and risk assessments and provide recommendations.
- Coordinate third party security assessments.
- Develop and implement security policies, standards and guidelines.
- Coordinate incident response activities.
- Report any identified security deficiencies to the Associate Provost and Chief Information Officer and appropriate Data Custodian.
- Coordinate security awareness training.

Information Technologies: Information Technologies has physical or logical possession of information. Responsibilities include:

- Provide support of systems.
- Use physical and logical access controls to protect information from unauthorized access, usage, modification or destruction.
- Administer access to information assets.
- Monitor systems for malicious events.

Users: Information users are personnel that are granted access to University and/or student information. User responsibilities include:

- Comply with the University Information Security Policy.
- Use the appropriate security controls for protecting information based on the associated risk.
- Reporting any suspicious activity.
- Reporting any lost, stolen or disclosed sensitive information.
- Use information only for the intended purpose.
- Ensure that non-public information is only distributed to authorized persons.
- Disposing of information in a secure manner.
- Access only information that they are authorized to access.

Compliance:
Anyone not in compliance with the information security policy or other applicable security policies could face loss of access to systems and assets or other sanctions as outlined in the HR Policies and student handbook.

F. HISTORY

Version	Review/Approval	Name	Date
2015	New document	Jim Miller	1/27/2015
2018	Update	Brian Rappach	3/08/2018

Other applicable policies and/or resources:

This document is part of the University's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary. Please refer to the other Xavier security policies below for further information or to the Xavier policies website for other relevant policies:

- Acceptable Use Policy
- Password policy
- Remote Access
- Vulnerability Management
- Data Classification
- Incident Response
- User Account Policy
- Information Technologies Change Management Policy