Applies to: faculty, staff, student employees, affiliated entities, agents, contractors, and volunteers.

INFORMATION SECURITY STANDARD (ISS)

Issued: v1.5 07/31/2017[1]

The Ohio State University Information Security Standard was developed to provide a definitive set of risk management objectives and security controls for all university information systems and assets under the university's control and for the people who access these systems. Use of this standard ensures that Ohio State consistently protects its information assets; satisfies legal, regulatory, and contractual requirements; and applies best practices for information security and risk management.

Table of Contents

[1] A history of *Information Security Standard* versions is available online.

1 About this Document

Accessibility: In several parts of this document, complex tables are used to organize information. An accessible version of the content is available at https://go.osu.edu/infosec-iss-accessible

2 Introduction

The *Information Security Standard* (ISS)[4] defines risk management objectives and specifies security controls that support Ohio State's *Information Technology Security Policy* (ITSP)[5]. The ISS is also linked to Ohio State's *Institutional Data Policy* (IDP)[6]. For more information about the ITSP and the IDP, see Appendix A Information Security and Risk Management Documentation.

The ISS defines 30 risk areas for the university. These risk areas are used to organize, measure, and manage information risk consistently across the university. The risk areas have been categorized according to eight business functions, to make them more accessible to managers. Each risk area definition includes a risk management objective, as well as a list of security controls to be used to meet the stated objective. The risk areas and security controls utilize a coding scheme to simplify cross-referencing between Ohio State's different information security and risk management documents.

The ISS is primarily based on the NIST SP 800-53[7] security standard and the *CPI-RISC Information Risk Framework*[8]. Additionally, the ISS references ISO 27002[9].

3 Compliance

All information systems and assets under Ohio State's control are expected to be managed in a way that complies with the ISS. Organizations are given the time between ISS updates and the end of the current program year to implement the new controls. Organizations must meet the Acceptable Level of Information Risk (ALIR) established for each risk area for the current program year. For more information about the ALIR and program years, see the Information Risk Management Program (IRMP)[10].

Additionally, organizations must comply with any applicable legal and regulatory requirements including those not referenced by the ISS.

An organization's level of compliance must be reported to the Information Security Advisory Board (SAB)[11], the Risk and Audit Committee, and Ohio State's Board of Trustees annually.

---

[2] The Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0) can be found at http://creativecommons.org/licenses/by-nc-sa/4.0/legalcode
[3] The Information Risk Management Program Documentation License (IRMPDL) can be found at https://go.osu.edu/infosec-irmpdl
[4] The *Information Security Standard* (ISS) can be found at https://go.osu.edu/infosec-iss
[5] The Information Technology Security Policy (ITSP) can be found at http://ocio.osu.edu/assets/Policies/ITSecurity.pdf
[6] The Policy on Institutional Data (IDP) can be found at https://go.osu.edu/idp
[7] National Institute of Standards and Technology (NIST) *Special Publication 800-53, Revision 4, Apr 2013: Security and Privacy Controls for Federal Information Systems and Organizations*. An information security standard developed by the US federal government that is widely used by federal, state, and local government organizations.
[8] *The Continuous Process Improvement–Risk, Information Security, and Compliance (CPI-RISC) Framework v1.3*, Feb, 2012. A business-oriented, standards-based approach to information security and risk management.
[9] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002:2005: *Information technology–Security techniques–Code of practice for information security management*. A well-respected definition of best practice for information security.
[10] The Information Risk Management Program (IRMP) can be found at https://go.osu.edu/infosec-irmp
[11] Information about the Information Security Advisory Board (SAB) can be found at https://go.osu.edu/infosec-sab

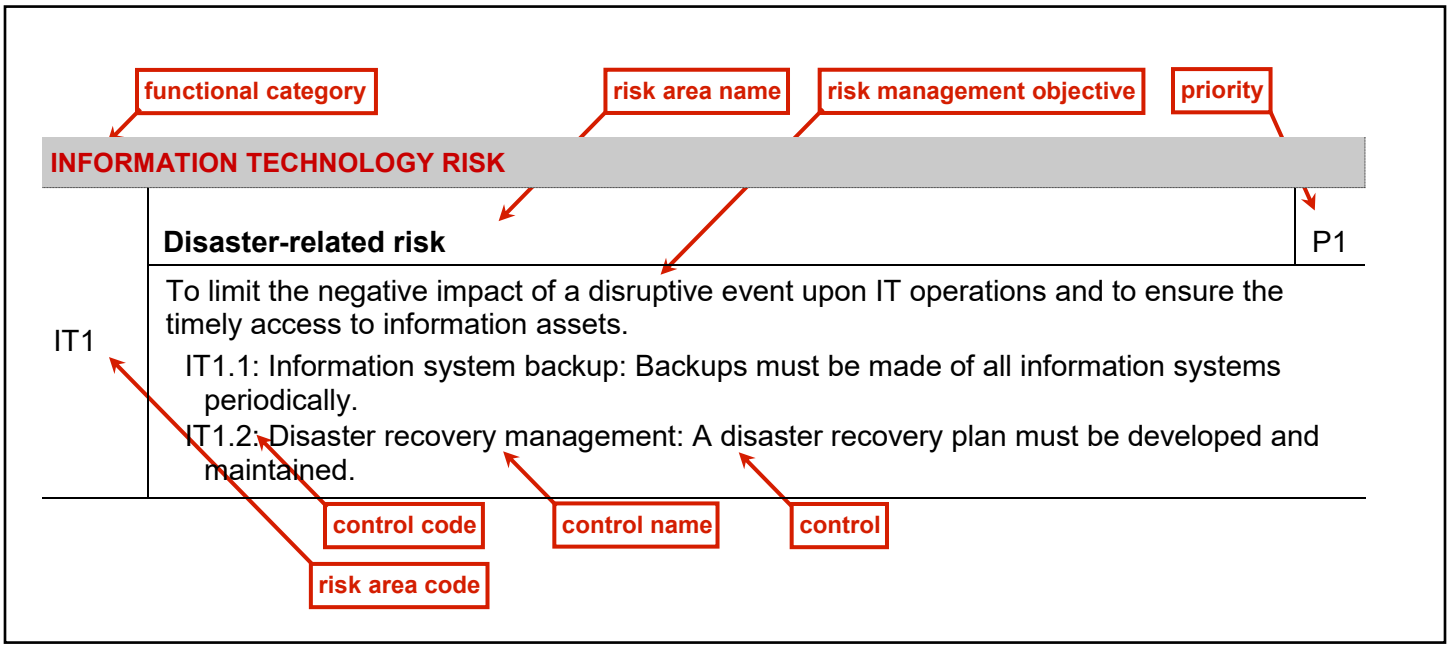
4 Exceptions

Organizations are required to track and self-manage exceptions when they determine they are non-compliant with the ISS. Non-compliance is defined as being unable to meet the ALIR for risk areas for the current program year.

Exceptions must be approved by an organization's senior management (e.g., VP or college dean) or their designee. Exceptions must be summarized and reported on a quarterly basis to the SAB.

5 Example

An example of a risk area definition from the ISS, with the component parts labeled:



6 Overview

The ISCR defines the control requirements for 30 risk areas, categorized by business function.

Code	Risk Area	Priority
MANAGEMENT RISK		
MGT1	Information risk management	P1
MGT2	Information security management	P2
MGT3	Compliance management	P1
MGT4	Business continuity management risk	P3
LEGAL RISK		
LEG1	Legal and regulatory compliance risk	P2
BUSINESS RISK		
BUS1	Finance system-related risk	P2
PURCHASING RISK		
PUR1	Contract management risk	P3
HUMAN RESOURCES RISK		
HR1	Employment risk	P2
FACILITIES RISK		
FAC1	Site-related physical risk	P2
FAC2	Workspace-related physical risk	P2
INSTITUTIONAL DATA RISK		
DAT1	Institutional data-related risk	P1
DAT2	Information access control-related risk	P1

Code	Risk Area	Priority
INFORMATION TECHNOLOGY RISK		
IT1	Disaster-related risk	P1
IT2	Infrastructure-related risk	P1
IT3	Network-related risk	P1
IT4	Server-related risk	P1
IT5	Identity-related risk	P1
IT6	Malicious software risk	P1
IT7	Application-related risk	P1
IT8	Development process-related risk	P2
IT9	Vendor management risk	P2
IT10	Client-related risk	P2
IT11	Mobile device-related risk	P2
IT12	Message service-related risk	P2
IT13	Web application-related risk	P2
IT14	Security incident management risk	P2
IT15	Storage media-related risk	P2
IT16	User-related risk	P2
IT17	Information asset management risk	P2
IT18	Software license management risk	P3

7 Standard

MANAGEMENT RISK		
MGT1	**Information risk management**	P1
	To ensure that information risks are identified and treated. MGT1.1: Risk assessment: A risk assessment must be performed periodically. MGT1.2: Risk management strategy: A risk management strategy must be developed and maintained.	
MGT2	**Information security management**	P2
	To ensure the information security program manages information risks. MGT2.1: Information security plan: An information security plan must be developed and maintained. MGT2.2: Information security roles: Information security role(s) must be assigned. MGT2.3: Information security resources: Information security resources must be allocated.	
MGT3	**Compliance management**	P1
	To ensure the risk management and information security programs effectively identify and manage information risks. MGT3.1: Security assessment: Security assessments must be performed periodically. MGT3.2: Penetration test: Penetration testing must be performed when required by regulation.	
MGT4	**Business continuity management risk**	P3
	To limit the negative impact of a disruptive event upon university operations. MGT4.1: Business continuity management: Business continuity plan(s) must be developed and maintained.	
LEGAL RISK		
LEG1	**Legal and regulatory compliance risk**	P2
	To ensure compliance with legal and regulatory requirements for risk management and information security. LEG1.1: Legal and regulatory review: Applicable legislation and regulations must be identified and reviewed periodically.	
BUSINESS RISK		
BUS1	**Finance system-related risk**	P2
	To prevent financial fraud. BUS1.1: Segregation of duties in operations: Segregation of duties must be verified in applicable financial systems. Note: Applicable financial systems include any information system responsible for entering, approving, or processing university financial transactions.	

PURCHASING RISK		
PUR1	**Contract management risk**	P3
	To ensure third party software product and information service vendors are contractually obligated to satisfy Ohio State's information security requirements. PUR1.1: Security-aware acquisition process: An acquisition process that includes security requirements must be used for the purchase of software products and information services. PUR1.2: Third party compliance: Contracts with third party software product and information service vendors must stipulate that their software and services satisfy the requirements of Ohio State's *Information Security Standard*. PUR1.3: Third party access: Contracts with third parties that need data- and/or network-access must require documented and approved access agreements. PUR1.4: Third party personnel compliance: Contracts with third parties that have personnel who will need access to Ohio State's internal information systems must require that their personnel review and comply with Ohio State's *Responsible Use of University Computing and Network Resources Policy.* PUR1.5: Third party personnel screening: Contracts with third parties that have personnel who will need access to institutional data must require that background checks are performed on their personnel before access is granted. PUR1.6 Third party termination: Digital identities must be disabled/deleted, access rights must be removed, and university information assets and institutional data must be retrieved and/or relinquished when third parties are terminated.	
HUMAN RESOURCES RISK		
HR1	**Employment risk**	P2
	To ensure that employee-related risk is managed throughout the employment lifecycle. HR1.1: Personnel screening: Employees must have a background check performed before being placed in positions where they will have access to institutional data. HR1.2: Personnel termination or transfer: Digital identities must be disabled/deleted, access rights must be removed, and university information assets and institutional data must be retrieved and/or relinquished when employees are terminated or transferred. HR1.3: Personnel corrective action: Appropriate corrective actions must be applied to employees who fail to comply with security requirements when required by regulation.	
FACILITIES RISK		
FAC1	**Site-related physical risk**	P2
	To prevent the theft of, tampering with, or destruction of information assets in university locations. FAC1.1: Building security: University locations must be equipped with physical access controls. Note: Information assets include infrastructure, information systems, software, or institutional data. University locations include buildings owned, managed, or leased by Ohio State.	
FAC2	**Workspace-related physical risk**	P2
	To prevent the theft of, tampering with, or destruction of information assets within workspaces. FAC2.1: Workspace security: Workspace locations must be equipped with physical access controls. Note: Information assets include infrastructure, information systems, software, or institutional data.	

INSTITUTIONAL DATA RISK		
DAT1	**Institutional data-related risk**	P1
	To ensure proper classification, labeling, and handling of institutional data. DAT1.1: Information categorization: Data must be categorized according to Ohio State's *Institutional Data Policy*. DAT1.2: Records management: University records must be managed according to records retention and disposition schedules. DAT1.3: Protected data storage: Data must be protected during storage as indicated by the data classification level. DAT1.4: Protected data transport: Data must be protected during transit as indicated by the data classification level. DAT1.5: Cryptography: University-approved cryptography must be used as indicated by the data classification level. DAT1.6: Data loss prevention: The presence of restricted institutional data must be detected on information systems and networks so the data can be protected. DAT1.7: Data integrity: Data integrity must be protected when required by regulation. Note: Data may be in digital or physical form.	
DAT2	**Information access control-related risk**	P1
	To ensure authorized access, use, and modification of institutional data as defined by Ohio State's *Institutional Data Policy.* DAT2.1: Access enforcement: Information systems must enforce access controls. DAT2.2: Access management: Users must receive only the minimum amount of access required to perform their work functions. DAT2.3: Separation of duties: User access and duties must be segregated when required by regulation.	
INFORMATION TECHNOLOGY RISK		
IT1	**Disaster-related risk**	P1
	To limit the negative impact of a disruptive event upon IT operations and to ensure the timely access to information assets. IT1.1: Information system backup: Backups must be made of all information systems periodically. IT1.2: Disaster recovery management: A disaster recovery plan must be developed and maintained.	

INFORMATION TECHNOLOGY RISK		
IT2	**Infrastructure-related risk**	P1
	To ensure university locations that house infrastructure are securely maintained. IT2.1: Infrastructure security: Infrastructure locations must be equipped with physical access controls. IT2.2: Infrastructure change management: Configuration changes must be made using a formal change control process. IT2.3: Emergency power: Electricity must be provided from an alternate source in case of an emergency. IT2.4: Fire protection: Fire detection and fire suppression systems must be maintained. IT2.5: Temperature and humidity control: Temperature and humidity must be monitored and controlled. Note: Infrastructure locations include data centers, server rooms, and technology rooms. A data center is an infrastructure location that houses one or more high availability information systems. A server room is an infrastructure location that houses one or more server systems. A technology room is an infrastructure location that houses voice and/or data network devices, wiring, or patch panels.	
IT3	**Network-related risk**	P1
	To ensure the secure operation of network devices and timely access to network services. IT3.1: Secure network device configuration: A predefined, secure configuration must be used. IT3.2: Least network device functionality: A minimal configuration must be used with only essential services enabled and configured. IT3.3: Network device change management: Configuration changes must be made using a formal change control process. IT3.4: Network device patch management: Software flaws must be identified and corrected. IT3.5: Legacy network device retirement: Current, vendor-supported software and firmware must be used. IT3.6: Network device logging: Network device and security events must be logged and monitored. IT3.7: Network device time synchronization: Network device clocks must be synchronized with a university-approved time source. IT3.8: Secure network remote access: Secure remote access must be enforced. IT3.9: Network boundary security: Secure network boundaries must be enforced. IT3.10: Network device vulnerability management: Network device vulnerabilities must be identified and managed. IT3.11: Network intrusion detection: The network must be monitored to detect unauthorized access or exploit. IT3.12: Network denial of service protection: The effects of denial of service attacks must be limited. IT3.13: Secure network device maintenance: Maintenance must be provided by authorized personnel without compromising device security or disclosing institutional data. IT3.14: Secure wireless network access: Secure wireless access must be enforced. Note: Network devices include routers, switches, firewalls, virtual network devices, and network components.	

INFORMATION TECHNOLOGY RISK		
IT4	**Server-related risk**	P1
	To ensure the secure operation of server systems and timely access to services. IT4.1: Secure server system configuration: A predefined, secure configuration must be used. IT4.2: Least server system functionality: A minimal configuration must be used with only essential services enabled and configured. IT4.3: Server system change management: Configuration changes must be made using a formal change control process. IT4.4: Server system patch management: Software flaws must be identified and corrected. IT4.5: Legacy server system retirement: Current, vendor-supported software and firmware must be used. IT4.6: Server system logging: System and security events must be logged and monitored. IT4.7: Server system time synchronization: System clocks must be synchronized with a university-approved time source. IT4.8: Secure server system remote access: Secure remote access must be enforced. IT4.9: Server system boundary security: Secure system boundaries must be enforced. IT4.10: Server system vulnerability management: Server system vulnerabilities must be identified and managed. IT4.11: Server system intrusion detection: Server systems must be monitored to detect unauthorized access or exploit. IT4.12: Server system denial of service protection: The effects of denial of service attacks must be limited. IT4.13: Secure server system maintenance: Maintenance must be provided by authorized personnel without compromising server system security or disclosing institutional data. IT4.14: Secure name and address resolution service: Name/address resolution services must be securely configured and managed. IT4.15: Secure database management: Database management services must be securely configured and managed. Note: Server systems include information systems that provide application, system, or network services to other information systems.	
IT5	**Identity-related risk**	P1
	To ensure the secure use and management of digital identities and that secure authentication processes are used. IT5.1: Identification and authentication: Information systems must require identification and authentication before providing access. IT5.2: Identity management: Digital identities must be securely managed. IT5.3: Credential management: Authentication credentials must be securely managed. IT5.4: Invalid login protection: Authentication processes must enforce a limit of consecutive invalid logon attempts. IT5.5: Secure identity server management: Identity management servers must be securely configured and managed. Note: Digital identities include accounts (e.g., user, service, and administrative), groups, and authentication credentials (e.g., passwords, tokens, and certificates).	

INFORMATION TECHNOLOGY RISK		
IT6	**Malicious software risk**	P1
	To ensure information systems and networks are protected from exploitation by malicious software. IT6.1: Anti-virus software: Anti-virus software must be used to detect and remove malicious software.	
IT7	**Application development-related risk**	P1
	To ensure secure operation of applications; that applications produce the correct results and perform only authorized transactions; and that data is not inadvertently exposed during processing. IT7.1: Input validation: Input data must be validated. IT7.2: Secure error handling: Error messages must be produced without exposing data. IT7.3: Segregation of duties in development: Segregation of duties must be implemented in applicable financial systems. IT7.4: Application banner: A system use notification banner must be displayed. IT7.5: Application boundary security: Secure application boundaries must be enforced using application-based tools. IT7.6: Application logging: Application and security events must be logged. IT7.7: Application session lock: Session locks must be enforced after periods of inactivity. IT7.8: Application denial of service protection: Applications must limit the effects of denial of service attacks. IT7.9: Application data protection: Application data must be protected during processing as indicated by the data classification level. IT7.10: Application developer training: Application developers must have the requisite skills to develop secure applications. IT7.11: Legacy development environment retirement: Current, vendor-supported development environments and tools must be used. Note: An application is a program or piece of software developed to perform a particular task. Application development is defined as writing a program or software to perform a particular task. An application developer is someone who writes a program or software to perform a particular task.	
IT8	**Development process-related risk**	P2
	To ensure the application development process produces secure applications. IT8.1: Application development process: A formal application development process must be used. IT8.2: Application development change management: Application and configuration changes must be made using a formal change control process. IT8.3: Application development third party compliance: Third-party agreements must require that external information service providers satisfy the requirements of Ohio State's *Information Security Standard*. IT8.4: Application development security: Internal and external connections to university information systems must be documented and approved.	
IT9	**Vendor management risk**	P2
	To ensure third party software product and information service vendors are meeting contractually defined service levels and Ohio State's information security requirements. IT9.1: Third party service management: Software and services provided by third party software product and information service vendors must be verified to ensure they satisfy the requirements of Ohio State's *Information Security Standard.*	

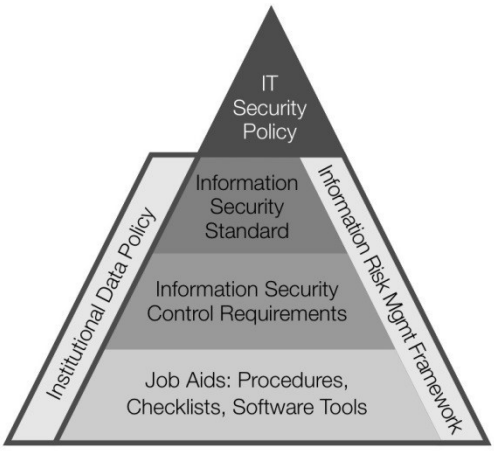
INFORMATION TECHNOLOGY RISK		
IT10	**Client-related risk**	P2
	To ensure the secure operation of client systems and applications. IT10.1: Secure client system configuration: A predefined, secure configuration must be used. IT10.2: Least client system functionality: A minimal configuration must be used with only essential services enabled and configured. IT10.3: Client system change management: Configuration changes must be made using a formal change control process. IT10.4: Client system patch management: Software flaws must be identified and corrected. IT10.5: Legacy client system retirement: Current, vendor-supported software and firmware must be used. IT10.6: Client system logging: System and security events must be logged and monitored. IT10.7: Client system time synchronization: System clocks must be synchronized with a university-approved time source. IT10.8: Secure client system remote access: Secure remote access must be enforced. IT10.9: Client system boundary security: Secure system boundaries must be enforced. IT10.10: Client system vulnerability management: Client system vulnerabilities must be identified and managed. IT10.11: Client system intrusion detection: Client systems must be monitored to detect unauthorized access or exploit. IT10.12: Secure client system maintenance: Maintenance must be provided by authorized personnel without compromising client system security or disclosing institutional data. Note: Client systems run general purpose operating systems (e.g., Microsoft Windows, Apple Mac OS X, Linux/UNIX) and don't host shared services to other information systems.	
IT11	**Mobile device-related risk**	P2
	To ensure the secure operation of mobile devices and applications. IT11.1: Basic secure mobile device configuration: Mobile devices accessing Ohio State's institutional data must be configured with a basic security configuration. *The following controls are required for mobile devices accessing, processing, storing, or transmitting restricted institutional data.* IT11.2: Mobile device or application management: Mobile devices must be securely managed (mobile device management (MDM)) or configured with a secure access application (mobile application management (MAM)). IT11.3: Mobile device or application change management: Configuration changes to the MDM or MAM system must be made using a formal change control process. IT11.4: Mobile device or application patch management: Software flaws in MDM or MAM systems and mobile devices must be identified and corrected. IT11.5: Legacy mobile device or application management: Current, vendor-supported MDM and MAM software must be used. IT11.6: Mobile device or application logging: System and security events from MDM or MAM systems must be logged and monitored. IT11.7: Secure mobile device configuration: A predefined, secure configuration must be used. IT11.8: Mobile device secure wipe: MDM systems must be able to be remotely erase and reset mobile devices; MAM systems must be able to remotely erase the MAM application data. IT11.9: Mobile device exploit detection: MDM or MAM systems must be monitored to detect unauthorized administrative access or exploit. Note: Mobile devices are portable systems that run embedded operating systems (e.g., Microsoft Windows RT and Windows Mobile, Apple iOS, Google Android, and Blackberry OS). These requirements apply to personally-owned as well as university-owned mobile devices that are being used to access institutional data.	

INFORMATION TECHNOLOGY RISK		
IT12	**Message service-related risk**	P2
	To ensure the secure operation of and timely access to messaging services. IT12.1: Message service anti-spam mechanism: Filter mechanisms must be used to detect and remove or block unsolicited bulk messages (e.g., spam or Spam over Internet Telephony (SPIT)). IT12.2: Message service anti-virus software: Anti-virus software must be used to detect and remove or block malicious messages or attachments. IT12.3: Secure message service: Messaging servers must be securely configured and managed. IT12.4: Secure message transmission: Messages must be transmitted using encryption as indicated by the data classification level. IT12.5: Secure Voice over Internet Protocol (VoIP): Voice over Internet Protocol (VoIP) services must be securely configured and managed. IT12.6: Secure collaborative computing: Collaborative computing must be securely configured and managed. IT12.7 Secure multi-function devices: Multi-function devices must be securely configured and managed. Note: Messaging services includes electronic mail, instant messaging, and Voice over Internet Protocol (VoIP) services. Collaborative computing includes applications, services, systems, or devices that allow two or more individuals to share information real time internal or external to the university (e.g., interactive whiteboard, screen sharing, and audio or video group conferencing). Multi-function devices incorporate the functionality of multiple devices in one to provide centralized document management/distribution/production while combining some or all of the following services (e.g., email, faxing, printing, copying, and scanning).	
IT13	**Web application-related risk**	P2
	To ensure the secure operation of web applications. IT13.1: Secure web sessions: Secure sessions must be enforced. IT13.2: Web application vulnerability management: Web application vulnerabilities must be identified and managed.	
IT14	**Security incident management risk**	P2
	To ensure a prompt and effective response to information security incidents. IT14.1: Security incident response plan: An incident response plan must be developed and maintained. IT14.2: Security incident response capability: Responses to information security incidents must be coordinated and managed. IT14.3: Security incident reporting: Security incidents must be reported promptly to Ohio State's Chief Information Security Officer.	

INFORMATION TECHNOLOGY RISK		
IT15	**Storage media-related risk**	P2
	To ensure that storage media and documents are used securely. IT15.1: Storage media physical security: Physical access to storage media and documents must be controlled. IT15.2: Storage media disposal: Storage media and documents must be disposed of securely. IT15.3: Storage media data protection: Institutional data must be encrypted on storage media as indicated by the data classification level. Note: Storage media includes optical media (e.g., CDs, DVDs), magnetic media (e.g., backup tapes, diskettes), storage drives (e.g., external drives, portable drives, or drives removed from information systems), and flash memory storage devices (e.g., SSDs or USB flash drives). Documents include paper documents, paper output, and photographic media.	
IT16	**User-related risk**	P2
	To ensure users are aware of security threats and behavior that makes them vulnerable and capable of performing information security-related roles. IT16.1: Information security awareness: All users must participate in information security awareness programs. IT16.2: Role-based information security training: All users must receive training to perform their information security roles and responsibilities.	
IT17	**Information asset management risk**	P2
	To ensure that information assets are identified so they can be managed securely. IT17.1: Information asset inventory: An inventory must be maintained of all university-owned network devices, information systems, and mobile devices.	
IT18	**Software license management risk**	P3
	To ensure that software is being used in compliance with license agreements and copyright law. IT18.1: Software license management: An inventory must be maintained of all software, software licenses, and related purchase records.	

Appendix A: Information Security and Risk Management Documentation

Ohio State's Enterprise Security group developed the Information Risk Management Program (IRMP) to manage information security risk to Ohio State's information systems and assets. The IRMP has produced a series of information security and risk management documents to assist organizations in understanding the program and implementing strategies to manage information risk. This appendix describes the purpose of and relationships between the various information security and risk management documents.



Ohio State Information Security and Risk Management Documentation Pyramid

Ohio State's *Information Technology Security Policy* (ITSP) establishes high-level information security requirements. The ITSP provides the mandate for the IRMP at Ohio State. It establishes the overall intent of the university to support and promote information security in all its practices. Additionally, the ITSP specifically delegates to the Office of the Chief Information Officer the responsibility to create new policies, standards, guidelines, requirements, and practices to support the intent of the policy and ensure information security.

The IRMP is also closely tied to Ohio State's *Institutional Data Policy* (IDP). The IDP defines different types of institutional data at Ohio State as well as high-level management and access requirements.

The Information Security Standard (ISS) defines 30 risk areas for the university. Each risk area includes a security objective, as well as a list of security controls to be used to meet the stated objective. These risk areas are used to organize, measure, and manage risk levels consistently across the university. The ISS takes its mandate from the ITSP and is tightly aligned with the IDP.

The *Information Security Control Requirements* (ISCR) provides detailed implementation guidance for each security control specified in the ISS. The ISCR could be interpreted as a more detailed version of the ISS. As such, a coding scheme makes it easy to cross-reference between the two documents. To better guide implementation efforts, the detailed control requirements in the ISCR are specified according to the level of institutional data being protected, as defined by the IDP.

The *Information Risk Management Framework* (IRMF) cross-references or maps the ISS security controls and ISCR control requirements to other security standards and regulations. As new information security regulations are created at the federal, state, or industry level, the IRMF will be expanded with additional appendices to document how the IRMP keeps Ohio State compliant with all relevant legislation and rules. The IRMF employs the same coding scheme utilized in the ISS and ISCR.

Over a multi-year period, the IRMP will develop job aids in the form of documentation (procedures, checklists, templates) and software tools as needed to support the implementation of the ISS and ISCR. Job aids will help organizations implement controls and control requirements effectively and efficiently.

Appendix B: Glossary

access controls:
the selective restriction of access to information or an information asset (e.g., access control lists, locks, or cryptography).

account:
a username used to identify a user of an information system or application. Ohio State defines different types of accounts: user account, sponsored guest account, shared accounts, service accounts, and administrative accounts.

administrative account:
an account with privileged access for the purpose of performing information system or application administrative tasks.

administrative system:
an information system that hosts multi-user applications; stores, processes, or transmits S2 (internal), S3 (private), or S4 (restricted) institutional data; or provides support for university business processes (e.g., PeopleSoft, eReports, or Operational Data Stores).

applicable financial system:
any system responsible for entering, approving, or processing university financial transactions.

application:
a program or piece of software developed to perform a particular task.

authentication:
verifying the identity of the user of an account.

authentication credential:
something used to establish or verify an identity (e.g., a password, token, or certificate).

authorization:
permission to access information or an information asset.

biometric authentication:
authenticating account access using a biometric device (e.g., fingerprint scanner, iris scanner, or facial recognition).

certificate:
a digital certificate is an electronic file that contains information (e.g., account attributes or authentication credentials) that can be used for authentication or authorization.

client system:
an information system that runs general purpose operating system software (e.g., Microsoft Windows, Apple Mac OS X, Linux/UNIX) and doesn't host shared services to other information systems.

collaborative computing:
an application, service, system, or device that allow two or more individuals to share information in real time, internal or external to the university (e.g., interactive whiteboard, screen sharing, and audio or video conferencing).

control:
an activity performed to meet a stated information risk management or security objective. Controls can be: administrative (e.g., policies, procedures, training), technical (e.g., hardware, software), or physical (e.g., door locks, closed circuit TV).

control code:
a 5-7 character alpha-numeric code used to simplify cross-referencing controls in Ohio State's different security documents.

control name:
a short, descriptive label for a control.

control requirement:
a set of specifications or instructions to be used to implement or guide the implementation of a control.

control requirement code:
7-10 character alpha-numeric code used to simplify cross-referencing control requirements in Ohio State's different security documents.

control requirement name:
a short, descriptive label for a control requirement.

critical system:
an information system that meets at least one of the criteria defined in DAT1.1.2 Critical system list.

data:
a piece of information in digital or physical form.

data center:
an infrastructure location that houses one or more high availability information systems.

data classification:
a formal categorization and labeling of Ohio State's institutional data based upon the sensitivity and regulatory privacy requirements for protecting the data. Ohio State's *Institutional Data Policy* defines four data classifications: public, internal, private, and restricted.

denial of service attack:
a category of resource exhaustion malicious software attack (e.g., account lock out, application

level connection/request flooding, corruption of data structures, and exception processing).

digital identity:
an account/userid (e.g., user, service, or administrative), group, or authentication credential.

document:
information in physical form (e.g., paper documents, paper output, or photographic media).

employee:
a university worker (e.g., faculty, staff, or student employees.)

functional category:
an area of management responsibility based on operational activity. Eight functional categories are defined: management, legal, business (finance), human resources, facilities, institutional data, and information technology.

high availability system:
an information system that meets at least one of the criteria defined in DAT1.1.3 High availability system list.

identity management server:
a server system that stores authentication credentials (e.g., Windows Active Directory domain controllers, RADIUS servers, or LDAP servers).

IDP:
Ohio State's Institutional Data Policy.

industry standard:
a security reference guide, security best practice publication, security benchmark, or security standard established and maintained by industry, academia, government agencies, or other organization in the public or private sector that is widely recognized.

information asset:
infrastructure, information systems, software, or institutional data.

Information Risk Management Framework (IRMF):
an Ohio State security document that cross-references or maps Information Security Standard and Information Security Control Requirements to other security standards and regulations.
Available at https://go.osu.edu/infosec-irmf

Information Security Control Requirements (ISCR):
an Ohio State security document that provides detailed implementation guidance for each security control specified in the Information Security Standard.
Available at http://go.osu.edu/infosec-iscr

Information Security Standard (ISS):
an Ohio State standard that defines information risk areas, security objectives, and security controls.
Available at http://go.osu.edu/infosec-iss

information system:
a client or server systems.

infrastructure location:
a data center, server room, or technology room.

institutional data:
information created, collected, maintained, transmitted, or recorded by or for the university to conduct university business. Defined by Ohio State's *Institutional Data Policy*.

internal institutional data:
an IDP data classification level; institutional data used to conduct university business and operations. It may only be accessed and managed by data users whose role, function, or assignment requires it. Unless otherwise indicated, internal is the default level for institutional data. Associated with security level S2.

IRMF:
Ohio State's *Information Risk Management Framework*.

ISCR:
Ohio State's *Information Security Control Requirements*.

ISS:
Ohio State's *Information Security Standard*.

lock:
keyed, combination, or university-approved offline key card reader locks.

maximum allowable downtime (MAD):
the amount of time an organization can be without an information system or application before it impacts a business process.

messaging service:
electronic mail, instant messaging, or Voice over Internet Protocol (VoIP) services.

mobile code:
a program, code, or object that can be migrated or moved from one information system or application to another (e.g., Java, JavaScript, ActiveX, Postscript, Shockwave movies, Flash animations, and VBScript).

mobile device:
a portable system that runs embedded operating system software (e.g., Microsoft Windows RT and

Windows Mobile, Apple iOS, Google Android, and Blackberry OS).

network device:
a router, switch, firewall, virtual network device, or network component.

personal data:
information created, collected, maintained, transmitted, or recorded by university owned devices, media, or systems that is personal in nature and not related to university business.

portable device:
a portable client system (e.g., laptop computer) or mobile devices (e.g., mobile phone, personal digital assistant (PDA), or tablet computer).

private institutional data:
an IDP data classification level; institutional data classified due to legal, regulatory, administrative, or contractual requirements; intellectual property or ethical considerations; strategic or proprietary value; and/or other special governance of such data. Access to and management of private data requires authorization and is only granted to those data users as permitted under applicable law, regulation, contract, rule, policy, and/or role. Associated with security level S3.

public institutional data:
an IDP data classification level; institutional data that is intended for public use and has no access or management restrictions. Associated with security level S1.

record:
a document, data, or set of data that is created or received in the course of an organization's business that has content, structure, fixity, context, and is maintained as evidence of an organization's activity. Institutional data may reside in university records, be used to produce university records, or may of itself be a university record.

recovery point objective (RPO):
the targeted period in which data may be lost from an information system or application due to a disruptive event.

recovery time objective (RTO):
the targeted duration of time for an information system or application to be restored to service after a disruptive event.

restricted institutional data:
an IDP data classification level; institutional data that requires the highest level of protection due to legal, regulatory, administrative, contractual, rule, or policy requirements. Access to and management of restricted data is strictly limited as unauthorized use or disclosure could substantially or materially impact the university's mission, operations, reputation, finances, or result in potential identity theft. Associated with security level S4.

risk area:
a collection of similar information risks that are grouped together.

risk area code:
a 3-4 character alpha-numeric code used to simplify cross-referencing risk areas in Ohio State's different security documents.

risk priority:
an information risk priority level for managing the specified risk area. Three risk priorities are defined: P1 (critical priority), P2 (high priority), and P3 (medium priority).

risk area name:
a short, descriptive label for a risk area.

risk management objective:
a measurable goal for handling information risk in a risk area.

S-level:
a security level, which links an institutional data classification with a level of effort to protect the institutional data. Four S-levels are defined: S1, S2, S3, and S4.

S1:
S level 1; associated with public institutional data.

S2:
S level 2; associated with internal institutional data.

S3:
S level 3; associated with private institutional data.

S4:
S level 4; associated with restricted institutional data.

security patch:
a software update, patch, or upgrade that impacts the security functions of an information system, mobile device, or network device.

server room:
an infrastructure location that houses one or more server systems.

server system:
an information systems that provides application, system, or network services to other information systems.

service account:
an account for non-interactive, automated information system or application access. Service accounts may have privileged access.

shared account:
an account that is shared among multiple users for limited, specific access for situations where the use of individual user accounts would not be possible practical. The account is sponsored by a university employee who is responsible for the account's activity.

sponsored guest account:
an account for accessing Ohio State information systems or applications for a user not associated with Ohio State. The account is sponsored by a university employee who is responsible for the guest's activity.

storage media:
optical media (e.g., CDs or DVDs), magnetic media (e.g., tapes or diskettes), disk drives (e.g., external, portable, or disk drives removed from information systems), or flash memory storage devices (e.g., SSDs or USB flash drives) used to store information.

technology room:
an infrastructure location that houses voice and/or data network devices, wiring, or patch panels.

third party attestation:
a certification provided by an external organization to independently verify the effectiveness of information security, including the Statements on Standards for Attestation Engagement (SSAE) 16 report (formerly Statements on Auditing Standards (SAS) 70) or ISO 27001 Information Security Management System (ISMS) certification.

token:
university-approved hardware- or software based access token that contain authentication credentials.

university location:
buildings owned, managed, or leased by The Ohio State University.

untrusted network:
a network not directly managed by an organization.

user account:
an account for interactive, user access to information systems or applications.