Washington State University Information Security Program

Revision History

Version No.	Date	Description	Author
1.0	12/16/2021	Initial Release	Tom Ambrosi

Approvals

DocuSigned by:

A6E5BDB60CF742C...

12/23/2021

Michael Walters, Interim Chief Information Security Officer

Date

DocuSigned by:

Sasi Kumar Pillay

8201AF15A292449...

12/28/2021

Sasi Pillay, Chief Information Officer

Date

1. Information Security Program Overview

1.1. Introduction

WSU is committed to protecting its employees, customers, partners, and constituents from all damaging acts – regardless of whether the acts are intentional or unintentional. Effective security is a team effort involving the participation and support of every entity that interacts with WSU systems, services, and information. Therefore, it is the responsibility of both WSU and third-parties to be aware of and adhere to WSU's cybersecurity and data protection requirements.

Protecting WSU information systems, services, and data is of critical importance. Commensurate with risk, security and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of systems, services, and information. Information security and privacy must include the appropriate controls and safeguards to protect against potential threats, as well as controls to ensure confidentiality, privacy, integrity, and availability of WSU information assets:

- **INFORMATION SECURITY** – The ability to ensure the confidentiality, integrity, and availability of institutional data held by WSU, regardless of its source or storage location.

- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.

- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.

- **INFORMATION PRIVACY** – the practice of ensuring freedom from intrusion into the private life or affairs of individuals when that intrusion results from undue or illegal gathering and use of data about that individual.

1.2. Purpose

The purpose of this document is to lay the groundwork for WSU's formal information security program and to provide a comprehensive high-level framework for: 1) providing effective procedural, administrative, technical, and physical safeguards for protecting information of WSU employees, students, alumni, partners, and constituents; 2) information security planning and execution of strategic, tactical, and operational plans and objectives; and 3) serving as a common foundation for all information security decisions and actions. Implementing consistent security and privacy controls across the WSU System will help ensure long-term due diligence in protecting the confidentiality, privacy, integrity, and availability of WSU systems, services, and information and to help WSU comply legal and regulatory obligations.

The formation of this program is driven by many factors, with key focus on cybersecurity risk and legal/regulatory compliance. The information security program, and the framework it operates under, describes how WSU operates and safeguards its systems, services, and information in order to reduce information security and privacy risk and to minimize the effect of potential incidents.   Information security and privacy policies, including their related control objectives, standards, procedures and guidelines, are necessary to support the management of information risks in daily operations. The development of the information security program and its associated documentation helps to provide due care to ensure WSU faculty, staff, students, constituents, and partners understand their day-to-day security responsibilities and the threats that could impact the WSU System.

1.3. Applicability and Scope

The Information Security Program applies to the entire WSU System:

- Employees, constituents, and 3rd parties including partners, contractors, sub-contractors, and their respective organizations supporting WSU business operations, wherever WSU information is stored, processed, transmitted, and shared including any 3rd parties contracted by WSU to handle, process, transmit, store, or dispose of WSU information; and
- Information, systems, services, activities, and assets owned, leased, controlled or used by WSU, partners, contractors or other 3rd parties on behalf of WSU that are within scope of the WSU Information Security Program

These policies do not supersede any other applicable law, regulation, higher-level WSU System directive or contractual or legal agreement in effect.

1.4. Mission

To ensure the confidentiality, integrity, availability, and privacy of WSU System information resources that are consistent with budgetary and regulatory constraints, and appropriately enables the University's mission and business functions with an acceptable level of information security and privacy risk.

1.5. Vision

- To integrate the WSU Information Security Program across the WSU System culture
- To develop and execute an Information Security Program that enables WSU System business units to carry out their roles in the management of information security and privacy risk

- To provide information security risk management oversight through continuous monitoring of security control implementations and the information security risk landscape

1.6. State, Federal and International Laws and Regulations

WSU is subject to a number of legislative and regulatory bodies and their respective policies, laws, regulations, and standards. All security strategies, policies, processes, architectures and subordinate elements will maintain compliance with all applicable laws and regulations, or seek exceptions as needed through any exceptions processes as defined in the applicable law or regulation.

Below are some of the major information security and privacy domains, laws, regulations and standards to which WSU is subject, in whole or in part:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- Washington's Uniform Health Care Information Act (RCW 70.02)
- Payment Card Industry Data Security Standard (PCI DSS)
- European Union General Data Protection Regulation (GDPR)
- Personal Information - Notice of Security Breaches (RCW 19.255.010; RCW 42.56.590)
- Federal Trade Commission (FTC) Red Flag Rule (Identity Theft Regulation)
- Regulations Governing the Protection of Research Data [e.g., Federal Information Security Management Act (FISMA), Controlled Unclassified Information (CUI), Washington State Uniform Trade Secrets Act (RCW 19.108)]
- Federal Acquisition Regulation (FAR) and Defense Acquisition Regulation Supplement (DFARS)
- Human Subjects Information Regulations
- National Security Information Regulations
- International Traffic in Arms Regulations (ITAR) (22 CFR 120-130)
- Export Administration Regulations (EAR) (15 CFR 730-774)
- Hazardous Materials

2. Information Security Program Structure

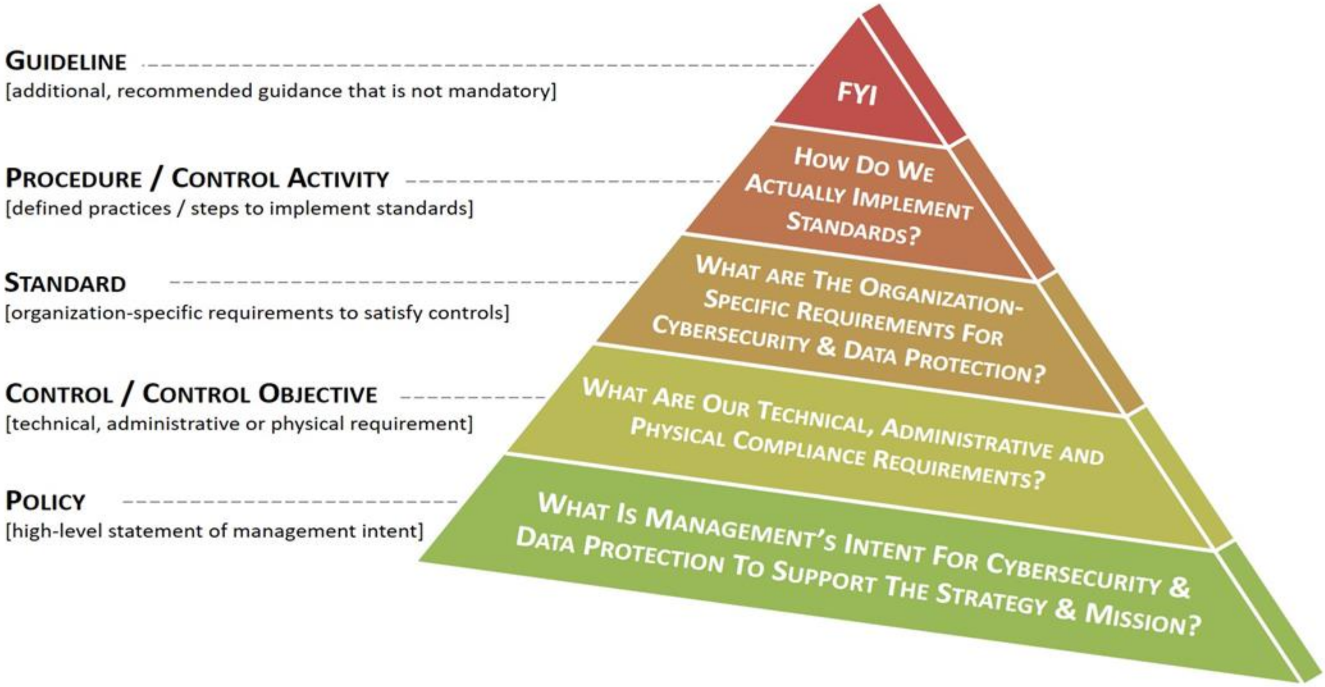
2.1. Program Objectives

The primary objective of this program is to provide management direction and support for information security activities and practices in accordance with WSU System business requirements and applicable policies, standards, laws, regulations, and legal requirements. This will accommodate the effective management of information security and privacy risks that are applicable in enterprise environments.

2.2. Documentation Hierarchy

The Information Security Program documentation consists of five core documentation types:

(1) Policies establish WSU's "management's intent" for cybersecurity and data protection requirements that are necessary to support WSU's overall strategy and mission;
(2) Controls / Control Objectives identify the technical, administrative and physical protection requirements that are generally tied to a law, regulation, industry framework or contractual obligation;
(3) Standards provide WSU-specific, quantifiable requirements for cybersecurity and data protection;
(4) Procedures (also known as Control Activities) establish the defined practices or steps that are performed to meet to implement standards and satisfy controls / control objectives; and
(5) Guidelines provide additional guidance that is recommended, but not mandatory.


GUIDELINE
[additional, recommended guidance that is not mandatory]
PROCEDURE / CONTROL ACTIVITY
[defined practices / steps to implement standards]
STANDARD
[organization-specific requirements to satisfy controls]
CONTROL / CONTROL OBJECTIVE
[technical, administrative or physical requirement]
POLICY
[high-level statement of management intent]
FYI
HOW DO WE ACTUALLY IMPLEMENT STANDARDS?
WHAT ARE THE ORGANIZATION-SPECIFIC REQUIREMENTS FOR CYBERSECURITY & DATA PROTECTION?
WHAT ARE OUR TECHNICAL, ADMINISTRATIVE AND PHYSICAL COMPLIANCE REQUIREMENTS?
WHAT IS MANAGEMENT'S INTENT FOR CYBERSECURITY & DATA PROTECTION TO SUPPORT THE STRATEGY & MISSION?

2.3. Information Security Framework

The NIST (National Institute of Standards & Technology) has been selected as the primary WSU information security framework due to: 1) it being recognized as the leading national information security framework; and 2) its alignment with federal regulatory requirements for the protection of WSU systems, services, applications, and data. In most cases, the use of the NIST framework provides a straight-forward alignment between the federal regulatory requirements and the NIST set of control objectives that can be implemented for compliance with federal regulations.

The use of the NIST framework as a reference guide for the WSU Information Security Program supports University efforts to provide a holistic, data-centric, and risk-based approach to securely designing, implementing, and maintaining WSU systems, applications, services, and information.

Below is a list of some of the documentation associated with the NIST framework that are referenced by or support WSU's Information Security Program:

- NIST 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
- Cybersecurity Maturity Model Certification (CMMC)
- NIST 800-30: *Guide for Conducting Risk Assessments*
- NIST 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST 800-39: *Managing Cybersecurity Risk: Organization, Mission and Information System View*
- NIST 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- NIST 800-64: *Security Considerations in Secure Development Life Cycle*
- NIST 800-122: *Guide to Protecting the Confidentiality of Personal Information (PI)*
- NIST IR 7298: *Glossary of Key Cybersecurity Terms*
- NIST SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability Act Security Rule
- NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0

Other international, federal, state, and industry requirements, standards and regulations that may be applicable to University systems and operations are listed in section 1.6 (State, Federal, and International Laws and Regulations).

3. Information Security Governance

Well-defined governance structures and models are essential to an effective Information Security Program. Well executed governance structures promote a collaborative approach for the development and execution of Information Security and Privacy programs.

The University IT governance structure is composed of three tiers. The President's Cabinet composes the highest-level tier and is the decision-making body for all major IT decisions and actions and ensures alignment with the WSU System mission, strategic plan and goals. The intermediary tier is the Information Technology Strategic Advisory Committee (ITSAC) and is responsible for developing and prioritizing significant opportunities for leveraging technologies University-wide and providing recommendations to the President's Cabinet. The final tier consists of several subcommittees one of which is the Information Security & Compliance Subcommittee. Recommendations developed by the subcommittees are proposed and evaluated by the ITSAC members.

More information on IT Governance at WSU, including Information Security & Compliance, can be found at:

https://its.wsu.edu/it-governance/

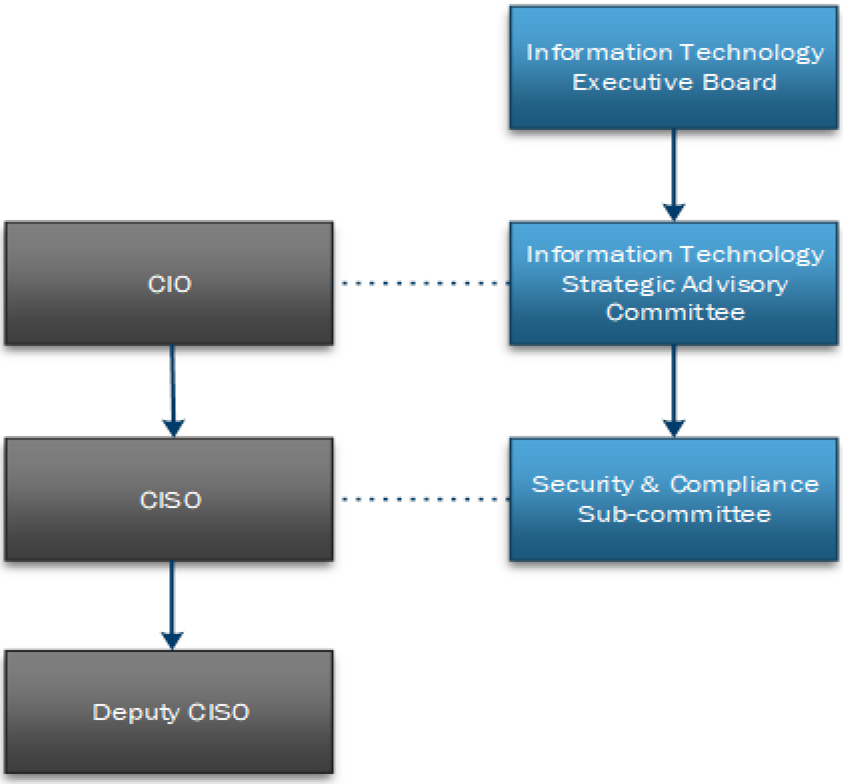
https://its.wsu.edu/it-executive-board/

3.1. Information Security Governance Structure

Governance of the University Information Security Program falls under the purview of the WSU System, Vice President and Chief Information Officer (CIO). Reporting to the CIO, the Chief Information Security Officer ("CISO") is responsible for overseeing the WSU System Information Security and Privacy Program. Under supervision of the CISO, oversight of the program is also delegated down to the Deputy CISO. The overall WSU System Information Technology Governance structure is depicted visually in Figure 1.

The CISO chairs the Information Security & Compliance Subcommittee (https://its.wsu.edu/subcommittees/#gov-sub-sac). The purpose of this committee is to advise the ITSAC and the CIO and to provide recommendations and guidance on institutional information security and privacy matters. The Information Security & Compliance Subcommittee has broad membership across the institution and is chartered to provide the following functions:

- Develop security program and plan.
- Make recommendations regarding security policies and standards.
- Provide security risk management.
- Gather and evaluate security metrics.
- Coordinate security assessments, audits, and compliance.
- Develop user security awareness and education programs.
- Focus on centralized vs. decentralized roles, responsibilities, authorities, and accountabilities.
- Review and recommend new security initiatives/solutions.
- Make funding recommendations.


Information Technology Executive Board
CIO
Information Technology Strategic Advisory Committee
CISO
Security & Compliance Sub-committee
Deputy CISO

Error! Reference source not found.

3.2. Governance Model

3.2.1. Roles, Responsibilities, and Authorities & Accountabilities

The CIO is the University official who is accountable for, and is authorized, to establish and maintain a WSU System Information Security Program *(see BPPM 87.01*). The CISO is the University official responsible for establishing and maintaining the WSU System Information Security Program *(see BPPM 87.01*) In alignment with the WSU System organizational structure and the distributed nature of how the University operates, executive heads of major University business units (e.g., vice presidents, chancellors, deans) are accountable for ensuring compliance with: 1) institutional information security and privacy related policies and standards; 2) contractual and data sharing agreements with third parties; and 3) all applicable information security and privacy related policies, standards, laws, and regulations *(see EP 37 WSU Information Security Policy*).

Other specific information security roles, responsibilities, authorities, accountabilities, and definitions are listed in BPPM 87.01 (WSU Information Security Roles, Responsibilities, and Definitions). Additional roles, responsibilities, authorities, and accountabilities may also be defined in policies listed in the Executive Policy Manual and the Information Security (87.00) section of the WSU Business Policy and Procedures Manual.

3.2.2. Policies

Policies are high level statements of management requirements from University executive leadership that are intended to influence decisions and to provide guidance for achieving desired University outcomes. The following lists contain University Information Security related polices that can be found in the WSU Executive Policy and Business Policies and Procedures Manuals:

WSU Executive Policy Manual

The Executive Policy Manual includes University policies approved by the appropriate governing body of University executive officers.

Executive Policy #4 Electronic Communication Policy (includes appropriate use of WSU information technology resources)

Executive Policy #8 University Data Policies

Executive Policy #16 University Network Policies

Executive Policy #37 WSU Information Security Policy

WSU Business Policies and Procedures Manual

The Business Policies and Procedures Manual (BPPM) is intended to guide and assist employees and administrators in the conduct of day-to-day administrative functions of the University.

BPPM 87.01 WSU Information Security Roles, Responsibilities, and Definitions

BPPM 87.05 Information System Account, Identity, and Authentication Management

BPPM 87.10 Mobile Device Management—WSU-Owned Mobile Devices

BPPM 87.11 BPPM 87.10 Mobile Device Management—Personally -Owned Devices

BPPM 87.15 Information Security Planning

BPPM 87.20 Security Assessment and Authorization

BPPM 87.25 Information Security Risk Assessment

BPPM 87.30 Configuration Management

BPPM 87.35 Wireless Local Area Network Management

BPPM 87.40 System and Information Integrity

BPPM 87.50 Audit and Accountability

BPPM 87.55 Information Security Incident Management and & Breach Notification

3.2.2.1. Policy Exceptions

Exceptions to this policy must be approved by the Office of the CIO, under the guidance of the appropriate information owner(s) and the University Chief Information Security Officer.

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exceptions. Approvals for policy exceptions are effective for a specified period of time and must be reviewed by the Office of the CIO annually.

3.2.2.2. Policy Enforcement

The Office of the Chief Information Officer (CIO) is responsible and has the authority for enforcing compliance with this policy.

3.2.2.3. Policy Violations

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable University policies and handbooks (e.g., the WSU Faculty Manual, the Administrative Professional Handbook, WAC 357-40 (civil service employees), applicable collective bargaining agreements, and the WSU Standards of Conduct for Students, WAC 504-26).

3.2.3. Control Objectives

The control objectives outlined in NIST SP 800-171 (revision 2) are the standard, base set of control objectives for the WSU System for protecting its systems and services, wherever WSU Confidential and/or Regulated information is stored, processed, transmitted, or shared. These control objectives contain the required administrative, technical, physical, and procedural controls and are detailed in the WSU Risk and Compliance Template. (if the template on the ITS webpage is not the current template, it will need to be replaced with the current template and the hyperlink updated)

The NIST Control families that contain the required control objectives are listed below:

- **AC - Access Control:** The AC Control Family consists of security requirements to determine when users have access to a system and their level of access, who has access to what assets, reporting capabilities like account management, system privileges, system logging, and remote access logging.
- **AT - Awareness and Training:** The AT Control Family requirements are specific to security training and procedures, including security training records.
- **AU - Audit and Accountability: The** AU control family consists of security controls related to audit capabilities. This includes audit policies and procedures, audit logging, audit report generation, and protection of audit information
- **CM - Configuration Management:** CM controls are specific to configuration management policies. This includes the requirements for baseline configurations to operate as the basis for future builds or changes to information systems, and information system component inventories.

- **IA - Identification and Authentication:** IA controls are specific to the identification and authentication policies. This includes the identification and authentication of organizational and non-organizational users and authentication policies for users, devices, and services, and credential management.
- **IR - Incident Response:** IR controls are specific to incident response policies and procedures. This includes incident response training, testing, monitoring, reporting, and response plan.
- **MA – Maintenance:** The MA controls in NIST 800-53 revision five detail requirements system, personnel, and tool maintenance.
- **MP - Media Protection:** The Media Protection control family includes controls specific to access, marking, storage, transport policies, sanitization, and defined media use.
- **PS - Personnel Security:** PS controls relate to the protection of personnel through position risk, personnel screening, termination, transfers, sanctions, and access agreements.
- **PE - Physical Protection:** The Physical and Environmental Protection control family is implemented to protect systems, buildings, and related supporting infrastructure against physical threats. These controls include physical access authorizations, monitoring, visitor records, emergency shutoff, power, lighting, fire protection, and water damage protection.
- **RA - Risk Assessment:** The RA control family relates to risk assessment policies and vulnerability scanning capabilities.
- **CA - Security Assessment and Authorization:** The Security Assessment and Authorization control family includes controls that supplement the execution of security assessments, authorizations, continuous monitoring, plan of actions and milestones, and system interconnections.
- **PL – Planning:** PL controls are specific to security planning policies and must address the purpose, scope, roles, responsibilities, management commitment, coordination among entities, and organizational compliance.
- **SC - System and Communications Protection:** The SC control family is responsible for systems and communications protection procedures. This includes boundary protection, protection of information at rest, collaborative computing devices, cryptographic protection, denial of service protection, and many others.
- **SI - System and Information Integrity:** The SI control family correlates to controls that protect system and information integrity. These include flaw remediation, malicious code protection, information system monitoring, security alerts, software and firmware integrity, and spam protection.

3.2.4. Contractual and 3rd Party Requirements

Information security and privacy protections required in vendor contracts and data sharing agreements with third parties are to be implemented for all applicable information assets for the systems/services covered by the 3rd party contract or agreement. This is to include all on-premise and other services being provided by 3rd parties. For 3rd parties that are providing services, current SSAE 18 (SOC 1 Type 2 and SOC 2 Type 2) reports, a Higher Education Cloud Vendor Assessment Tool (HECVAT) report, a completed Washington State Office of Cybersecurity Design Review Checklist, or comparable, 3rd party information security assessment report needs to be provided.

Third parties that store, process, and or transmit WSU Confidential and Regulated data are required to complete an Information Services (IS) Review Questionnaire for Technology Contracts and Purchases *(see BPPM 70.24).* Third parties that store, process, and or transmit WSU Internal information are also required to have a signed contract or data sharing agreement with WSU. The WSU Data Security and Confidentiality Terms and Conditions contains the required data protection and sharing provisions.

3.2.5. Standards

- WSU Information System Audit Accountability Standard
- WSU Authentication Management Standard
- WSU Account and Identity Management Standard
- WSU Tiered Administration Standard
- WSU Role Based Access Control Standard
- WSU Endpoint Security Standard
- WSU Boundary Device Standard
- WSU Cloud Acceptable Use Matrix (PDF)
- WSU Cloud Acceptable Use Matrix (PDF)
- WSU Information Security Compliance Template

3.2.6. Procedures (or Processes)

BPPM 87.55 Information Security Incident Management and & Breach Notification (link to be provided when approved and published by ITSAC & the President's Cabinet)

BPPM 60.00 Personnel Policies & Procedures (https://policies.wsu.edu/prf/index/manuals/60-00-personnel/)

BPPM 60.74 Employee Departure Procedures (https://policies.wsu.edu/prf/index/manuals/60-00-personnel/60-74-employee-departure-procedures/)

Employee Departure Checklist (https://policies.wsu.edu/prf/documents/2017/10/60-74-departure-checklist.pdf/)

BPPM 70.24 Acquisition of Computer Equipment, Services, or Software (https://policies.wsu.edu/prf/index/manuals/70-00-purchasing/70-24-acquisition-computer-equipment-services-software/)

BPPM 30.64 Identity Theft Prevention Program (https://policies.wsu.edu/prf/index/manuals/30-00-contents/30-64-identity-theft-prevention-program/)

BPPM 30.64 Processing University Contracts (https://policies.wsu.edu/prf/index/manuals/30-00-contents/30-64-identity-theft-prevention-program/)

BPPM 85.00 Computing and Telecommunications (https://policies.wsu.edu/prf/index/manuals/85-00-computing-telecommunications/)

BPPM 90.00 University Records (http://policies.wsu.edu/prf/index/manuals/90-00-records/)

BPPM 50.20 Access to University Facilities (http://policies.wsu.edu/prf/50-00-contents/50-20-access-university-facilities/)

BPM 20.00 University Property (http://policies.wsu.edu/prf/index/manuals/20-00-property/)

https://policies.wsu.edu/prf/index/manuals/bppm-table-contents/). Where no WSU System process or procedures exist, Information Owners, as Executive heads of major WSU System Business Units, are accountable for developing appropriate processes or procedures for the implementation of all information security and privacy policies.

3.2.7. Guidelines

- Security Tips for International Travel (PDF)
- WSU Cloud Computing Guideline (PDF)
- Guidelines for Developing a Security Assessment Plan (PDF)

3.2.8. Shared Responsibility

Protecting University systems, services, and information regardless of where they reside, is a team effort and requires everyone to do their part according to their roles, delegated authorities, and responsibilities. A shared responsibility model defines divisions of responsibilities for the protection of the various elements that make up an entire system or service ecosystem, from the lowest level of information technology infrastructure to include physical datacenter environments and cabling infrastructure, to applications and data and managing access to those applications and data. For on-premise systems and services, the divisions of responsibility may be divided between various University business units, to include central ITS units and/or one or more administrative or academic business units. For 3rd party or cloud Software-as-a-Service solutions, the division of responsibility will be divided among the 3rd party or cloud provider and the appropriate University business units. Regardless of whether systems and services reside on-premises or at a 3rd party or vendor site, the responsibility for security and privacy compliance lies with the appropriate WSU business unit(s) that are responsible for the deployment, use, management, and maintenance of the particular system or service.

3.2.9. Cyber Liability Insurance

WSU currently carries Cyber Liability insurance on an annual basis. WSU's current policy holder is Brit Ltd (Brit) and the actual insurer or underwriter is Lloyd's, London. The current policy period is from March 1, 2021 to March 2, 2022. The aggregate limit of liability for the policy period is $5,000,000 with a general retention limit of $100,000 per claim and an aggregate retention of $200,000 per policy period.

Areas of coverage include privacy and security breach response services, notification services and identity protection services, PCI DSS assessments coverage, cyber extortion, business income loss and digital asset restoration, multimedia liability, and cyber crime.

Specific limits, sub-limits, and retentions for individual coverages vary and are listed in the document, “WSU 21-22 Cyber Binder – Brit.pdf”.

4. Review Cycle

The Office of the CIO is to review this program document at least every three years or on as-needed basis due to changes to changes in 1) WSU System requirements and/or business operating environments, 2) legal or regulatory requirements, 3) or information security frameworks.

5. Appendix A: Glossary

5.1. Acronyms

Acronym	Definition

5.2. Terms

Term	Definition

6. Appendix B: Works Cited

1. ComplianceForge, LLC
2. NIST Special Publication 800-171 Revision 2 *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
3. NIST Special Publication 800-37 Revision 2 Risk Management Framework for Information Systems and Organizations