Trina Zanow, Division Administrator
Chief Information Officer

State of Wisconsin

IT Security Policy Handbook

Effective Date: July 1, 2022

TABLE OF CONTENTS

STATUTORY AUTHORITY

Wisconsin State Statutes Chapter 16 SUBCHAPTER VII INFORMATION TECHNOLOGY describes the responsibilities and duties of the Department of Administration (DOA) related to setting policies and procedures for the administration of information technology (IT) services.

16.971 Responsibilities of department. (2) The department shall:

(a) Ensure that an adequate level of information technology services is made available to all executive branch agencies by providing systems analysis and application programming services to augment agency resources, as requested. The department shall also ensure that executive branch agencies, other than the board of regents of the University of Wisconsin System, make effective and efficient use of the information technology resources of the state. The department shall, in cooperation with the executive branch agencies, establish policies, procedures, and planning processes, for the administration of information technology services, which executive branch agencies shall follow. The policies, procedures and processes shall address the needs of agencies, other than the board of regents of the University of Wisconsin System, to carry out their functions. The department shall monitor adherence to these policies, procedures, and processes.

(k) Ensure that all state data processing facilities develop proper privacy and security procedures and safeguards.

16.973 Duties of the department. The department shall:

(3) Facilitate the implementation of statewide initiatives, including development and maintenance of policies and programs to protect the privacy of individuals who are the subjects of information contained in the databases of agencies, and of technical standards and sharing of applications among executive branch agencies and any participating local governmental units or entities in the private sector.

(4) Ensure responsiveness to the needs of executive branch agencies for delivery of high-quality information technology processing services on an efficient and economical basis, while not unduly affecting the privacy of individuals who are the subjects of the information being processed by the department.

(5) Utilize all feasible technical means to ensure the security of all information submitted to the department for processing by executive branch agencies, local governmental units, and entities in the private sector.

OVERVIEW

The State of Wisconsin IT Security Policy Handbook has been developed to provide a baseline of executive branch IT security policies and controls. This handbook contains an explanation of terms for guiding principles, policies, standards, procedures, and key components of the IT security approach and governance process. Included in the handbook are all current security policies with links to associated standards, cross-referenced to the NIST Special Publication 800-53, Revision 5 guidelines. NIST Special Publication 800-53, Revision 5 guidelines define recommended baseline security controls for governmental organizations. As provider of the State of Wisconsin consolidated data center services, which involve a multitude of federal and state regulatory requirements, DOA has adopted the NIST Special Publication 800-53, Revision 5, as the foundational framework for executive branch IT security policies and standards.

SCOPE

All State of Wisconsin executive branch agencies, excluding the board of regents of the University of Wisconsin System, are expected to adhere to these policies. (Non-executive branch agencies are also strongly encouraged to adopt and adhere to these polices.) As needed to address business requirements, agencies can employ more rigorous policies and standards in relation to agency-specific applications and processes.

ROLES AND RESPONSIBILITIES

- Chief Information Officer (CIO)
    - Ensures that DOA drafts, finalizes, and promulgates executive branch IT security policies.
    - Reviews and approves any DOA-specific IT Security policies.

- Chief Information Security Officer (CISO)
    - Develops and administers the DOA/Division of Enterprise Technology (DET) IT Security Program.
    - Formulates any DOA-specific IT security standards.
    - Provides guidance to management in interpreting federal, state, and local security laws and requirements.

- Administrative Officers (AO)
    - Ensures the implementation of IT security policies within their respective executive branch agencies.
    - Provides governance oversight of executive branch IT security policies.

- Deputy Chief Information Security Officer, Division of Enterprise Technology, Bureau of Security
    - Researches and develops necessary IT security policies, standards, and procedures.
    - Maintains the IT security policies, standards, and procedures review schedule for DOA/DET.
    - Publishes updates to the DOA/DET Portal as necessary.
    - Facilitates the processing of any requests for exceptions to executive branch IT security policies and standards.
    - Provides IT security compliance consulting support as it relates to regulatory requirements and security industry best practices.

COMPLIANCE

The executive branch IT security policies contained in this handbook will take effect upon approval by the Department of Administration Secretary's Office and subsequent publication. The DOA/DET Bureau of Security will ensure a review of the handbook at least once every year to ensure relevancy.

If compliance with particular policies or related standards is not feasible or technically possible, or if deviation is justifiable to support a business function, agency representatives can request an exception through the DOA/DET Bureau of Security Exception Procedure (https://detcc.wi.gov/security/Pages/securitypoliciesstandards.aspx).

COORDINATION AMONG AGENCIES

The State of Wisconsin DOA/DET consolidated data center's customer base is subject to multiple regulatory requirements designed to ensure the effective implementation of appropriate IT security measures. Listed below are the primary regulatory requirements that DOA/DET and its executive branch agency customers are subject to:

- Centers for Medicare and Medicaid Services (CMS) - Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges, Version 2 (MARS-E)
- Criminal Justice Information Services (CJIS) Security Policy, Version 5.9
- Family Educational Rights and Privacy Act (FERPA) Compliance
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- Payment Card Industry – Data Security Standard (PCI-DSS)
- Social Security Administration (SSA) Technical System Security Requirements
- Wisconsin State Statutes Chapter 16.971

The DOA/DET consolidated data center shares responsibility with executive branch agency customers for safeguarding assets and information including, but not limited to, Federal Tax Information (FTI), Protected Health Information (PHI), and Personally Identifiable Information (PII). DOA/DET employs security mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across executive branch agency boundaries.

DOA/DET may designate selected controls as "agency-defined." Implementation of some controls may need to be done in partnership between DOA/DET and the regulated state agency. However, the executive branch state agency maintains primary responsibility for ensuring it is completed.

Note: All regulatory publications map to the security controls in NIST Special Publication 800-53, Revision 5, which is used as the primary reference point by the DOA/DET, Bureau of Security for IT security policies, standards, and procedures.

ENFORCEMENT/SANCTIONS

Enforcement of the security policies applying to executive branch state agencies will be conducted at the agency level. All determinations regarding appropriate sanctions for violations of executive branch IT security policies will be facilitated by agency Human Resources management.

IT SECURITY GOVERNANCE – TERMINOLOGY AND DEFINITIONS

The following definitions apply to this document:

- **Guiding Principles**
  - Over-arching statements that convey the philosophy, direction, or belief of an organization.
  - Guiding principles are not policies but serve as guideposts in the formulation of security policies and procedures.
  - Guiding principles serve to "guide" people in making the right decisions for an organization.

- **Policies**
  - A formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, rules, and objectives for a specific subject area.
  - Specific policies are created to mitigate risks within multiple categories that include, but are not limited to, information security, data privacy, and regulatory compliance.
  - As noted above, multiple regulatory requirements mandate that the State of Wisconsin. "Develop, document, and disseminate…" security policies in specific areas to executive branch agencies.

- **Standards**
  - Actions or rules designed to support and conform to a policy.
  - A standard should make a policy more meaningful and effective. Standards are usually written to describe the requirements for various technology configurations (e.g., mobile devices, type in use for encryption, firewall settings).
  - A standard must include one or more accepted specifications for hardware, software, or behavior.

- **Procedures**
  - Procedures are the specific instructions for aligning with standards and policies, consisting of a series of steps taken to accomplish an end-goal policy statement.
  - Procedures are important to achieving policy goals. The policies define what is to be protected and the procedures outline how to implement the standards or how to fulfill the requirements and expectations of the policies.
  - Regulatory requirements are to "develop, document, and disseminate … procedures to facilitate the implementation…" of associated policies.

ALIGNMENT WITH IT GOVERNANCE

The following will ensure consistent oversight for all IT security guiding principles, policies, standards, and procedures.

- Executive branch IT security policies that constitute a baseline for state agencies will be presented to the Department of Administration Secretary's Office for review and approval.
- Executive branch IT security guiding principles, policies, and standards will be published by DOA.
- Agencies can employ more rigorous policies and standards in relation to agency-specific applications and processes, as needed to address business requirements.
- All agencies will maintain and disseminate to employees procedures that accomplish the end-goal executive branch IT policies and standards (or, in the case of instances where the agency employs more rigorous policies and standards in relation to *agency-specific* applications and processes, the agency will maintain and disseminate procedures that accomplish the agency's more rigorous policies and standards).

COMMUNICATION

- All approved security guiding principles, policies, and standards that apply to executive branch

agencies will be published to the DOA/DET Customer Portal.

- Policies, standards, and procedures will be communicated to all appropriate personnel upon approval.
- Executive branch IT security policies and standards will be incorporated into the State of Wisconsin IT Security Awareness Training Program.

SECURITY POLICY AND STANDARDS REVIEW AND MAINTENANCE

The following processes will be implemented to ensure compliance to regulatory requirements.

- Executive branch agency IT security policies and standards will be reviewed a minimum of annually. (When specific language in either the IT Policy Handbook or standards documents can be modified to add clarity or resolve any discrepancies between policies and standards, this often can be done immediately and does not have to be incorporated into a formal review process. Please contact the DOA/DET Bureau of Security if you see areas where language in the IT Policy Handbook or standards can be improved in this manner.)

- DOA/DET Bureau of Security personnel will:
    - Document policy review and approval procedures;
    - Maintain the policy review schedule;
    - Publish IT security guiding principles, policies, standards and procedures that apply to executive branch agencies to the DOA/DET Customer Portal;
    - Maintain a single repository for documentation that applies to all executive branch agencies; and
    - Coordinate the review and tracking of exception requests to executive branch agency IT security policies and standards.

IT SECURITY POLICIES

AC-01 Access Control Policy

Purpose

The Access Control Policy is for managing security and privacy risks associated with user account management, access enforcement and monitoring, insufficient separation of duties, lack of adherence to the principle of least privilege and remote access security. The related access control standards will facilitate the implementation of security best practices for logical security, account management, and remote access.

Policy

System Access may only be granted upon receipt of an approved agency "Access Request Form" from an authorized submitter. The granting of access privileges must follow the principle of least privilege, be appropriate to job role, and commensurate with appropriate account management assignments (user, privilege, and system accounts).

Standards and associated NIST security control recommendations

- Access Control Standard (100)
  - AC-2 Account Management
  - AC-3 Access Enforcement
  - AC-4 Information Flow Enforcement
  - AC-5 Separation of Duties
  - AC-6 Least Privilege
  - AC-7 Unsuccessful Logon Attempts
  - AC-8 System Use Notification
  - AC-11 Device Lock
  - AC-12 Session Termination
  - AC-14 Permitted Actions Without Identification or Authentication
  - AC-17 Remote Access
  - AC-18 Wireless Access
  - AC-19 Access Control for Mobile Devices
  - AC-20 Use of External Systems
  - AC-21 Information Sharing
  - AC-22 Publicly Accessible Content
- Access Control for Remote Access Standard (101)
- Access Control for Wireless Access Standard (102)
- Access Control for Mobile Device Security (103)
- Identification and Authentication Standard (160)
- Data Classification Standard (191)
- Personnel Security Standard (220)
  - PS-4 Personnel Termination

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- Internal Revenue Service Special Publication 6103
- NIST Special Publication 800-53, Revision 5

AT-01 Security Awareness and Training Policy

Purpose

The Security Awareness and Training Policy is for managing risks from a lack of IT security awareness, communication, and training through the establishment of an effective security awareness and education program. The security awareness and education program will train agency personnel, contractors, and interns on security best practices and concepts.

Policy

Executive branch agencies will develop and/or procure and make available online security awareness training with a focus on security best practices, role-based security and responsibilities for all agency personnel, contractors, and interns to ensure an understanding of agency security policies and current IT security best practices. It is a requirement that any individual issued a computer account by an executive branch state agency – including employees, contractors, interns, volunteers, and business partners – receive security awareness training and disclosure training. This training will take place upon issuance of the computer account by the agency and include refresher security awareness training annually.

Standards and associated NIST security control recommendations

- Security Awareness and Training Standard (110)
    - AT-2 Literacy Training and Awareness
    - AT-3 Role-Based Training
    - AT-4 Training Records

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- Internal Revenue Service Special Publication 6103
- NIST Special Publication 800-53, Revision 5

AU-01 Audit and Accountability Policy

Purpose

The Audit and Accountability Policy is for managing risks from inadequate event logging and transaction monitoring. The related audit and accountability standard ensures the implementation of security best practices regarding event logging and transaction monitoring and the retention of audit evidence.

Policy

The audit and log functions of executive branch agencies must enable the detection and capture of event data of unauthorized access to sensitive and classified information, and information requiring regulatory protection. Audited events must be reviewed regularly and where possible when unauthorized access events have been identified.

Auditing must be enabled to the greatest extent necessary to capture access, modification, deletion, and movement of sensitive and classified information by unique username/ID. Event storage retention must remain in compliance with regulatory requirements and be supported with an appropriate amount of storage for the required retention period. Time-stamp capabilities must be synchronized for monitoring auditable devices and events.

Standards and associated NIST security control recommendations

- Audit and Accountability Standard (120)
    - AU-2 Event Logging
    - AU-3 Content of Audit Records
    - AU-4 Audit Log Storage Capacity
    - AU-5 Response to Audit Logging Process Failures
    - AU-6 Audit Record Review, Analysis, and Reporting
    - AU-7 Audit Record Reduction and Report Generation
    - AU-8 Time Stamps
    - AU-9 Protection of Audit Information
    - AU-11 Audit Record Retention
    - AU-12 Audit Record Generation

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

CA-01 Security Assessment and Authorization Policy

Purpose

The Security Assessment and Authorization Policy is for managing risks from inadequate security assessments, authorization, and continuous monitoring of executive branch agency information assets through the establishment of an effective security assessment program. This policy and the associated standard help to implement security best practices regarding security assessments, authorization, and continuous monitoring.

Policy

Develop and conduct periodic security assessment(s), which may include vulnerability and penetration tests, which evaluate and document security measures in place on all critical agency IT systems and system environments. The agency will define the appropriate timeframes for conducting these assessments based on security best practices and regulatory compliance (if applicable). Security assessment reports must be formally documented and reported to agency management, with a description of the assessment controls being evaluated, associated findings/observations, definition of the assessment environmental landscape, remediation activities, owner, and identification of the assessment team.

Standards and associated NIST security control recommendations

- Security Assessment and Authorization Standard (130)
    - CA-2 Control Assessments
    - CA-3 Information Exchange
    - CA-5 Plan of Action and Milestones
    - CA-6 Authorization
    - CA-7 Continuous Monitoring
    - CA-9 Internal System Connections

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5
- Payment Card Industry – Data Security Standard (PCI-DSS)

CM-01 Configuration Management Policy

Purpose

The Configuration Management Policy is for managing risks from system changes impacting baseline configuration settings, system configuration, and security based on the principle of "least functionality." The configuration management standards will help document, authorize, manage, and control system changes impacting information system components within the control of the executive branch agency.

Policy

To ensure a secured and consistent implementation of protection mechanisms, baseline configurations and supporting procedures for all agency applications must be developed, documented, and maintained. These baselines should follow best practices, e.g., those outlined by the Center for Internet Security (CIS) Benchmarks or the United States Government Configuration Baseline (USGCB). Regulatory requirements must be reviewed at least annually, and updates made to agency systems environments as needed.

Standards and associated NIST security control recommendations

- Configuration Management Standard (140)
  - CM-2 Baseline Configuration
  - CM-3 Configuration Change Control
  - CM-4 Impact Analyses
  - CM-5 Access Restrictions for Change
  - CM-6 Configuration Settings
  - CM-7 Least Functionality
  - CM-8 System Component Inventory
  - CM-9 Configuration Management Plan
  - CM-11 User-Installed Software
  - CM-12 Information Location

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

CP-01 Contingency Planning Policy

Purpose

To ensure continuation of operations, the Contingency Planning Policy is for managing risks from information asset disruptions, failures, and disasters through the establishment of effective contingency planning procedures. The contingency planning procedures ensure the implementation of security best practices regarding business continuity and disaster recovery plans.

Policy

All essential executive branch agency systems will be identified and documented within a formal contingency plan, along with procedures that define recovery objectives, restoration priorities, success metrics that include recovery time and recovery point objectives, roles and responsibilities, and contact lists. The contingency plan must be reviewed on an annual basis.

Standards and associated NIST security control recommendations

- Contingency Planning Standard (150)
  - CP-2 Contingency Plan
  - CP-3 Contingency Training
  - CP-4 Contingency Plan Testing
  - CP-6 Alternate Storage Site
  - CP-7 Alternate Processing Site
  - CP-8 Telecommunications Services
  - CP-9 System Backup
  - CP-10 System Recovery and Reconstitution

Compliance References

- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

Purpose

The Identification and Authentication Policy is for managing risks from user access (agency, non-agency) and authentication into executive branch agency information assets through the establishment of an effective identification and authentication program.

Policy

Individuals attempting access to state agency-managed networks (internal or external) or enterprise systems must be uniquely identified and authenticated before establishing a connection to any state-managed network.

Standards and associated NIST security control recommendations

- Access Control Standard (100)
  - AC-2 Identification and Authentication (Agency Users)
- Identification and Authentication Standard (160)
  - IA-2 Identification and Authentication (Agency Users)
  - IA-3 Device Identification and Authentication
  - IA-4 Identifier Management
  - IA-5 Authenticator Management
  - IA-6 Authenticator Feedback
  - IA-7 Cryptographic Module Authentication
  - IA-8 Identification and Authentication (Non-Agency Users)
  - IA-11 Re-authentication
  - IA-12 Identity Proofing

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

Purpose

The Incident Response Policy is for establishing guidelines for the identification, response, reporting, assessment, analysis, and follow-up to all suspected information security incidents. The agency's related information security response procedures help to ensure the security, confidentiality, integrity and availability of electronic information and the automated systems that contain it and the networks over which it travels.

Policy

This policy requires the definition of a consistent operational approach for responding to identified or reported IT security incidents. An executive branch agency must develop formal Incident Response Procedures that include the areas of IT security incident event identification, notification, containment, eradication, and recovery.

Executive branch agencies must:

- Train personnel, including contractors, in their incident response roles.
- Test the incident response capability at least annually.
- Require personnel to report suspected security, privacy, and supply chain incidents by following their agency incident response procedure.
- Develop an incident response plan that provides the agency with a roadmap for implementing its incident response capability.

Standards and associated NIST security control recommendations

- Incident Response Standard (170)
  - IR-2 Incident Response Training
  - IR-3 Incident Response Testing
  - IR-4 Incident Handling
  - IR-5 Incident Monitoring
  - IR-6 Incident Reporting
  - IR-7 Incident Response Assistance
  - IR-8 Incident Response Plan

Compliance References

- Criminal Justice Information Services (CJIS) Security Policy, Version 5.9
- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5
- Payment Card Industry – Data Security Standard (PCI-DSS)

MA-01 System Maintenance Policy

Purpose

The System Maintenance Policy is for managing risks associated with information asset maintenance and repairs. The related System Maintenance standard and development of procedures will ensure the implementation of security best practices regarding system maintenance and repairs.

Policy

Executive branch agencies will develop formal and documented procedures to ensure consistent practices regarding the planning, scheduling, performing, documenting, reviewing, and recording of maintenance and repairs for all agency-controlled IT system components in accordance with manufacturer or vendor specifications, or in accordance with any relevant DOA/DET requirements for information system maintenance.

Personnel performing maintenance on the information system components must have appropriate identification and/or been previously authorized by the executive branch agency.

Standards and associated NIST security control recommendations

- System Maintenance Standard (180)
  - MA-2 Controlled Maintenance
  - MA-3 Maintenance Tools
  - MA-4 Non-Local Maintenance
  - MA-5 Maintenance Personnel
  - MA-6 Timely Maintenance

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

Purpose

The Media Protection Policy is for managing risks from media access, media storage, media transport, and media protection through the establishment of effective Media Protection standards and procedures. The related media protection standard and procedures will ensure the implementation of security best practices and control activities regarding media usage, storage, and disposal (media being digital or non-digital media).

Policy

Access controls to all sensitive and confidential information must restrict access to both digital and non-digital media to only authorized personnel using physical and logical access control mechanisms. Protection mechanisms will be implemented to protect sensitive or regulated information whether at rest or in transit. Media protection is required during the life cycle of the storage medium until such time the media has been physically destroyed or sanitized using only approved destruction equipment, techniques, and procedures.

Standards and associated NIST security control recommendations

- Media Protection (190)
  - MP-2 Media Access
  - MP-3 Media Marking
  - MP-4 Media Storage
  - MP-5 Media Transport
  - MP-6 Media Sanitization

Compliance References

- Criminal Justice Information Services (CJIS) Security Policy, Version 5.9
- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5
- Payment Card Industry – Data Security Standard (PCI-DSS)

PE-01 Physical and Environmental Protection Policy

Purpose

The Physical and Environmental Protection Policy is for mitigating the risks from physical security and environmental threats through the establishment of an effective physical security and environmental control standard and procedures. The physical security and environmental controls program help protect its IT assets from physical and environmental threats whether internal or external.

Policy

Physical access to DOA/DET infrastructure facilities where protected/restricted information and system assets or infrastructure reside will be restricted to authorized personnel based upon the principle of least privilege. This policy applies to both DOA and executive branch agency personnel. For visitors, documentation must be retained to capture the individual's identification by showing formal identification documentation – e.g., driver's licenses and state or government IDs containing photo. All personnel granted access to restricted buildings must display appropriate identification badges above the waist.

As provider of the State of Wisconsin consolidated data center, DET must protect environmental control equipment (HVAC), monitoring systems and required power cabling, control boxes, and piping from inappropriate access, tampering, damage and destruction. Further protection of the infrastructure components must include emergency shutoff, power, lighting, fire protection (detection and suppression), temperature and humidity controls, and water damage.

Executive branch state agencies must also utilize appropriate physical and environmental protection mechanisms at all alternate work sites where protected/restricted information resides.

Standards and associated NIST security control recommendations

- Physical and Environment Protection Standard (200)
    - PE-2 Physical Security Access Authorizations
    - PE-3 Physical Access Control
    - PE-4 Access Control for Transmission
    - PE-5 Access Control for Output Devices
    - PE-6 Monitoring Physical Access
    - PE-8 Visitor Access Records
    - PE-9 Power Equipment and Cabling
    - PE-10 Emergency Shutoff
    - PE-11 Emergency Power
    - PP-12 Emergency Lighting

- PE-13 Fire Protection
- PE-14 Environmental Controls
- PE-15 Water Damage Protection
- PE-16 Delivery and Removal

Compliance References

- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5
- Payment Card Industry – Data Security Standard (PCI-DSS)

PL-01 Security Planning Policy

Purpose

The Security Planning Policy is for managing risks from inadequate security planning through the establishment of an effective security planning program. The related security planning standard and procedures ensure the implementation of security best practices for security planning, preparation, and strategy development.

Policy

Executive branch agencies must develop and maintain IT security and privacy plans for moderate and high-risk systems or when required by Federal regulatory requirements (if applicable). The plans should include security and privacy measures taken to protect all information assets located at alternate agency work sites and the agency's responsibilities in assuring the security of information in transit to and from the State of Wisconsin consolidated data center. Agencies planning to deploy new applications or major upgrades to existing applications will conduct a security risk analysis. If the agency identifies security issues that may require modification to the agency security or privacy plan, the agency has the responsibility to consult with the DET Bureau of Security to review the proposed modifications.

Standards and associated NIST security control recommendations

- Planning (210)
  - PL-2 System Security and Privacy Plans
  - PL-4 Rules of Behavior

Compliance References

- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5
- Payment Card Industry – Data Security Standard (PCI-DSS)

PS-01 Personnel Security Policy

Purpose

The Personnel Security Policy is for managing risks from personnel screening, termination, management, and third-party (contractors, vendors, interns) access, through the establishment of effective security planning procedures. The personnel security procedures ensure the implementation of security best practices regarding personnel screening, termination, transfer, and management.

Policy

Executive branch agencies are required to document and utilize appropriate personnel screening and/or background checks prior to initiating employment of new hires. Similarly, executive branch agencies are required to document and utilize appropriate security measures and checklists at the time an employee separates from the agency. The personnel security requirement for each type of role in the agency must be formally documented and monitored for individual compliance. Third-party vendors or contractors working for the agency are also subject to established agency security policies. Access agreements between the executive branch agency and vendor/contractors must be reviewed and updated on a periodic basis defined and documented by the agency.

Standards and associated NIST security control recommendations

- Personnel Security Standard (220)
    - PS-2 Position Risk Designation
    - PS-3 Personnel Screening
    - PS-4 Personnel Termination
    - PS-5 Personnel Transfer
    - PS-6 Access Agreements
    - PS-7 External Personnel Security
    - PS-8 Personnel Sanctions

Compliance References

- Criminal Justice Information Services (CJIS) Security Policy, Version 5.9
- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5
- 2017 Wisconsin Act 154

Purpose

The Risk Assessment Policy is established so that the impact of an information system compromise can be reduced in an efficient manner. The related risk assessment standard and procedures will ensure the implementation of security best practices regarding the identification of known vulnerabilities to State of Wisconsin information assets.

Policy

Timely risk assessments of the executive branch agency's business functions, information assets and systems are required to protect against potential threats and vulnerabilities in the areas of confidentiality, integrity, and availability of protected and restricted information and of information and systems necessary in carrying out State responsibilities. Assessments consist of steps to:

- Determine business requirements and potential business impacts from compromise;
- Identify the impact that could occur from an information system compromise;
- Determine areas of vulnerabilities;
- Identify threats and the likelihood of compromise; and
- Initiate appropriate remediation activities to remediate or mitigate vulnerabilities and threats.

Standards and associated NIST security control recommendations

- Risk Assessment Standard (230)
  - RA-2 Security Categorization
  - RA-3 Risk Assessment
  - RA-5 Vulnerability Monitoring and Scanning
  - RA-7 Risk Response
  - RA-9 Criticality Analysis
- Data Classification Standard (191)

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5
- NIST Special Publication 800-60

SA-01 System and Services Acquisition Policy

Purpose

The System and Services Acquisition Policy is for managing risks from third party products and service providers, through the establishment of effective third-party risk management plan. The related system and services acquisition standard and procedures helps to ensure the implementation of security best practices regarding the acquisition of systems and services from third-party providers.

Policy

The acquisition of systems (assets) and services from third-party providers are subject to a security assessment review by the executive branch agency to address compliance to established security policies, procedures, and standards prior to the actual purchase or contracting of services. Regulatory compliance must be maintained post implementation and throughout the life cycle of the product or service contracts being acquired.

Standards and associated NIST security control recommendations

- System and Services Acquisition Standard (240)
    - SA-2 Allocation of Resources
    - SA-3 System Development Life Cycle
    - SA-4 Acquisition Process
    - SA-5 System Documentation
    - SA-8 Security and Privacy Engineering Principles
    - SA-9 External System Services
    - SA-10 Developer Configuration Management
    - SA-11 Developer Testing and Evaluation
    - SA-22 Unsupported System Components

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

SC-01 System and Communication Protection Policy

Purpose

The System and Communications Protection Policy is for managing risks from vulnerable system configurations, denial of service, data communication, and transfer. The associated system and communications protection standard and procedures help implement security best practices regarding system configuration, data communication, and transfer as they relate to the confidentiality, integrity, and availability of information.

Policy

Sensitive and confidential agency information, whether at rest or in-transit, must be protected from accidental or intentional threats that could corrupt, modify, delete, or disclose that information. Controls must consider threats from denial of service, attacks against network boundaries, transmission mechanisms, network disconnects, collaborative computing devices, other critical system components, multi-function devices, and printers.

Standards and associated NIST security control recommendations

- System and Communications Protection Standard (250)
    - SC-2 Separation of System and User Functionality
    - SC-4 Information in Shared System Resources
    - SC-5 Denial of Service Protection
    - SC-7 Boundary Protection
    - SC-8 Transmission of Confidentiality and Integrity
    - SC-10 Network Disconnect
    - SC-12 Cryptographic Key Establishment and Management
    - SC-13 Cryptographic Protection
    - SC-15 Collaborative Computing Devices and Applications
    - SC-17 Public Key Infrastructure Certificates
    - SC-18 Mobile Code
    - SC-23 Session Authenticity
    - SC-28 Protection of Information at Rest

Compliance References

- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

SI-01 System and Information Integrity Policy

Purpose

The System and Information Integrity Policy is for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling. The related system and information integrity standard and procedures help the executive branch agency implement security best practices regarding system configuration, security, and system and information error handling processes and procedures.

Policy

Executive branch agency business systems must:

- Identify, report, and correct information system flaws.
- Test software updates related to flaw remediation for effectiveness and potential side effects on organizational information assets before installation.
- Incorporate flaw remediation and error handling into the organizational configuration management process.
- Employ, configure and update malicious code protection mechanisms at information asset entry and exit points and at workstations or mobile computing devices on the network to detect and eradicate malicious code.

Sensitive and regulated information must maintain its integrity and be protected against compromise by potential threats and vulnerabilities. All critical security event mechanisms must have event detection monitoring, capturing, and reporting of violation events. Security violation event records are required to be logged and retained based on current regulatory requirements applicable to the agency applications (currently seven years for IRS, 10 years for CMS).

Standards and associated NIST security control recommendations

- System and Information Integrity Standard (260)
    - SI-2 Flaw Remediation (includes patch management)
    - SI-3 Malicious Code Protection
    - SI-4 System Monitoring
    - SI-5 Security Alerts, Advisories, and Directives
    - SI-8 Spam Protection
    - SI-12 Information Management and Retention

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

PM-01 Program Management Policy

Purpose

The Information Security Program was developed in response to the following requirements:

- Wisconsin Statutes Chapter 16 assigns responsibility of proper privacy and security procedures/safeguards; information security planning; threat-mitigation; and resource development to the Department of Administration.
- NIST Special Publication 800-53 Revision 5, which defines baseline security controls for governmental organizations, requires identification and documentation of the senior-level official(s) responsible for information security programs.

Policy

Management of the State's Information Security Program is provided by:

- The DOA Secretary's Office reviews and approves executive branch state agency IT security policies. The executive branch IT Policy Handbook will provide a baseline of security policies and controls throughout executive branch agencies. DOA/DET will publish and maintain these policies and related standards.
- As needed to address business requirements, agencies can employ more rigorous policies and standards in relation to agency-specific applications and processes.
- DOA/DET will ensure that the executive branch state agency IT security policies and standards are reviewed at least annually. Any proposed policy changes, based on DOA/DET review and agency input, will be brought back to the DOA Secretary's Office.
- The DOA/DET Chief Information Officer (CIO) is the designated official assigned with the responsibility to create an information security program that applies to all executive branch state agencies (PM-2).
- The DOA/DET Chief Information Security Officer (CISO) is the designated official assigned with:
  - executing the information security program that applies to all executive branch state agencies;
  - developing the mission and program priorities;
  - documenting policies and standards to address IT and information security needs; and
  - securing resources (including assistance from internal and external personnel and IT assets) to coordinate, develop, implement, and maintain the information security program (PM-2, PM-11, PM-13).

Standards and associated NIST security control recommendations

- Program Management Standard (500)

- AC-1 Access Control
- AT-1 Awareness and Training
- AU-1 Audit and Accountability
- CA-1 Security Assessment and Authorization
- CM-1 Configuration Management
- CP-1 Contingency Planning
- IA-1 Identification and Authentication
- IR-1 Incident Response
- MA-1 Maintenance
- PT-1 PII Processing and Transparency
- MP-1 Media Protection
- PL-1 Planning
- PS-1 Personnel Security
- RA-1 Risk Assessment
- SA-1 System and Services Acquisition
- SC-1 System and Communication Protection
- SI-1 System and Information Integrity
- PM-1 Program Management
- SR-1 Supply Chain Risk Management

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

PT-01 Personally Identifiable Information Processing and Transparency Policy

Purpose

The Personally Identifiable Information Processing and Transparency Policy is for managing risks from inadequate collection, processing, and maintenance of personally identifiable information. The related personally identifiable information processing standard ensures the implementation of security best practice regarding processing personally identifiable information.

Policy

Processing of PII must be restricted to only that which is authorized. Executive branch agencies must take steps to ensure that personally identifiable information is only processed for authorized purposes, including training agency personnel on the authorized processing of personally identifiable information and monitoring and auditing agency use of personally identifiable information. Individuals must be provided with notification about and give consent for the processing of PII.

Standards and associated NIST security control recommendations

- Personally Identifiable Information Processing and Transparency Standard (270)
    - PT-2 Authority to Process Personally Identifiable Information
    - PT-3 Personally Identifiable Information Processing Purposes
    - PT-4 Consent
    - PT-5 Privacy Notice
    - PT-7 Specific Categories of Personally Identifiable Information

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

SR-01 Supply Chain Risk Management Policy

Purpose

The Supply Chain Risk Management Policy is for managing risks from inadequate protection against supply chain threats. The related supply chain risk management standard and procedures help the executive branch agency implement security best practices regarding security or privacy risks to the supply chain.

Policy

Executive branch agencies must take steps to ensure supply change security and manage potential risks to the supply chain. Supply chain risk management activities include identifying and assessing risks, determining appropriate risk response actions, developing supply chain risk management plans to document response actions, and monitoring performance against plans.

Standards and associated NIST security control recommendations

- Supply Chain Risk Management Standard (280)
    - SR-2 Supply Chain Risk Management Plan
    - SR-3 Supply Chain Controls and Processes
    - SR-4 Provenance
    - SR-5 Acquisition Strategies, Tools, and Methods
    - SR-6 Supplier Assessments and Reviews
    - SR-7 Supply Chain Operations Security
    - SR-8 Notification Agreements
    - SR-9 Tamper Resistance and Detection
    - SR-10 Inspection of Systems or Components
    - SR-11 Component Authenticity
    - SR-12 Component Disposal

Compliance References

- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/16)
- NIST Special Publication 800-53, Revision 5

APPENDICES

Appendix A – ACRONYMS

Common IT security abbreviations adopted from NIST Special Publication 800-37, Revision 5 and the State of Wisconsin

- APT Advanced Persistent Threat
- CIO Chief Information Officer
- CISO Chief Information Security Officer
- CJIS Criminal Justice Information Services
- CPO Chief Privacy Officer
- DOA/DET Department of Administration – Division of Enterprise Technology
- DNS Domain Name System
- DOA Department of Administration
- DoD Department of Defense
- FAR Federal Acquisition Regulation
- FEA Federal Enterprise Architecture
- FERPA Family Educational Rights and Privacy Act
- FICAM Federal Identity, Credential, and Access Management
- FIPS Federal Information Processing Standards
- FISMA Federal Information Security Management Act
- HIPAA Health Insurance Portability and Accountability Act
- HSPD Homeland Security Presidential Directive
- IPsec Internet Protocol Security
- IRS Internal Revenue Service
- LACS Logical Access Control System
- NIST National Institute of Standards and Technology
- NSA National Security Agency
- OMB Office of Management and Budget
- OPSEC Operations Security
- PCI-DSS Payment Card Industry Data Security Standard
- PII Personally Identifiable Information
- PIV Personal Identity Verification
- PKI Public Key Infrastructure
- RMF Risk Management Framework
- SCADA Supervisory Control and Data Acquisition
- SP Special Publication
- TCP/IP Transmission Control Protocol/Internet Protocol
- USB Universal Serial Bus
- USGCB United States Government Configuration Baseline
- VoIP Voice over Internet Protocol
- VPN Virtual Private Network

Appendix B – Glossary/Definitions

Common IT security terms adopted from NIST Special Publication 800-37, Revision 5 and the State of Wisconsin

Term	Definition
Access Control	Security control designed to permit authorized access to an IT system or application.
Accessible	Information arranged, identified, indexed, or maintained in a manner that permits the custodian of the public record to locate and retrieve the information in a readable format within a reasonable time.
Authentication	Verification of the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
Availability	The extent to which information is operational, accessible, functional, and usable upon demand by an authorized entity (e.g., a system or user).
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Configuration Management	The process of keeping track of changes to the system, if needed, approving them.

Term	Definition
Contingency Plan	A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and the successful continuity of operations in an emergency.
Control	An action taken to enhance the likelihood that established goals or objectives will be achieved (in the context of this handbook, generally an action taken to reduce risk).
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted.
Executive Branch Agencies	Administrative departments, executive agencies, boards, and councils of the State of Wisconsin executive branch of government as described in the State of Wisconsin Blue Book. For the purpose of these enterprise security policies, the UW System is not included, though the UW System is in the executive branch.
Identification	The process that enables a user described to an IT system or service.
Digital Media	A form of electronic media where data are stored in digital (as opposed to analog) form.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Term	Definition
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Incident Response	The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
Information Asset	Information and systems that provide value to an agency or organization.
Integrity	Integrity is the protection of information from tampering, forgery, or accidental changes. It ensures that messages are accurately received as they were sent, and computer errors or non-authorized individuals do not alter information.
Intrusion detection	Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
Least Functionality	The organization configures information systems to provide only essential capabilities, and disables unused or unnecessary components of information systems to prevent unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling.

Term	Definition
Least Privilege	Granting users, programs, or processes only the access they specifically need to perform their business task and no more.
Multifactor Authentication	Using more than one of the following factors to authenticate to a system: Something you know (e.g., user-ID, password, personal identification number (PIN), or passcode); something you have (e.g., a one-time password authentication token, 'smart card'); something you are (e.g., fingerprint, retina scan).
Privileged Account	A privileged account is an account which provides increased access and requires additional authorization. Examples include a network, system, or security administrator account.
Remote Access	The connection of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information.
Risk	The probability that a particular threat will exploit a particular vulnerability of the system.
Risk Assessment	The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.
Security (IT)	Measures and controls that protect IT systems/information against denial of access and unauthorized (accidental or intentional) disclosure, modification, or destruction of ITs and data. IT security includes consideration of all hardware and/or software functions.

Term	Definition
System	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, applications, and communications.
Threat	A potential circumstance, entity, or event capable of exploiting vulnerability and causing harm. Threats can come from natural causes, human actions, or environmental conditions. A threat does not present a risk when there is no vulnerability.
User	Any State Entity, federal government entity, political subdivision, their employees or third-party contractors or business associates, or any other individuals who are authorized by such entities to access a system for a legitimate government purpose.
Vulnerability	A weakness that can be accidentally triggered or intentionally exploited.

Appendix C – Review, Revision, Approval Log

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
1.0	10/15/18	Draft executive branch state agency IT Security Policy Handbook submitted to and approved by the IT Executive Steering Committee	Reviewer: ITESC Author: DOA/DET	10/15/18
1.0	10/29/19	Reviewed with Agency Security Officers and feedback collected. Planning for making revisions.	Bureau of Security	
2.0	10/06/20	Draft executive branch state agency IT Security Policy Handbook submitted to Agency Security Officers for review	Reviewer: WI ISAC Author: DOA/DET	
3.0	11/03/20	Draft Executive Branch IT Security Policy Handbook submitted to Agency Security Officers, Agency IT Directors, DOA Secretary's Office and Agency Administrative Officers for review.	Reviewer: WI ISAC, ITDC, DOA Secretary's Office, AOs Author: DOA/DET/BOS	11/11/20
4.0	4/01/2022	Draft Executive Branch IT Security Policy Handbook submitted to the Agency Security Officers and Agency IT Directors for review.	Reviewer: WI ISAC, Enterprise IT Author: DOA/DET	6/24/2022
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				