State of Wisconsin
Department of Administration
Division of Enterprise Technology
SECURITY

State of Wisconsin

Department of Administration

Division of Enterprise Technology

Information Technology (IT)

Security Policy Handbook

Table of Contents

STATUTORY AUTHORITY

Wisconsin State Statutes Chapter 16 SUBCHAPTER VII INFORMATION TECHNOLOGY describes the responsibilities and duties of the Department of Administration 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 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 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 agencies and any participating local governmental units or entities in the private sector.

(4) Ensure responsiveness to the needs of 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 agencies, local governmental units and entities in the private sector.

OVERVIEW

The IT Security Policy Handbook contains an explanation of terms for guiding principles, policies, standards, procedures, and key components of the Division of Enterprise Technology (DET) IT Security Governance Process. Included in the handbook are all current DET IT security policies with links to associated procedures and standards cross-referenced to the NIST 800-53 Version 4 guidelines which define recommended baseline security controls for governmental organizations.

The handbook will be used to manage the portfolio of DET IT security policies, procedures and standards to ensure a single source for all governance documents, and to ensure governance documents are reviewed and approved according to regulatory or statutory requirements. Additionally, operating procedures, guidelines and templates will ensure a consistent delivery of security practices to meet the policy requirements. Each policy defined in handbook will contain additional details on purpose, policy statement, and links to procedures and standards that further facilitate the implementation of the policies.

Governance documents are to be reviewed annually at a minimum, by an approved document owner. Each of the IT security policies, procedures and standards will be assigned to an owner who is responsible for reporting changes to the documents and to conduct periodic document reviews.

The DET IT security policies contained in this document provide a baseline of security requirements for current and planned consolidated information technology services and the establishment of standards for new IT (hardware and software) initiatives.

SCOPE

All employees, contractors, vendors and interns employed by or providing services to DET are subject to the IT security guidelines, policies, procedures and standards listed in this handbook. The IT Security Policy Handbook applies to all individuals with access to, or who operate in support of DET services and information.

This handbook covers all infrastructure components (hardware, software and facilities) under DET management at all locations throughout the State of Wisconsin. Although not required, executive branch agencies may choose to adopt all or portions of this DET IT Security Policy Handbook.

MANAGEMENT COMMITMENT

As provider of the State of Wisconsin consolidated data center services with a multitude of federal and state regulatory requirements, DET has adopted the NIST 800-53 publication version 4 as the framework for its IT security policies. The DET management team is committed to implementing, maintaining and enforcing the DET IT security policies in this handbook to ensure the protection of sensitive and confidential information from compromise as it relates to availability, confidentiality, and integrity.

ROLES AND RESPONSIBILITIES

- Chief Information Officer (CIO)
  - Ensures that the Agency creates and implements an Agency-wide IT security policy
  - Approval and review of DET IT security policies
- Chief Information Security Officer (CISO)
  - Develops and maintains the DET IT security policies
- Agency CIO Steering Committee (ACSC)
  - Ensures the implementation of IT security policies within their respective Agencies
  - Provides governance oversight to published DET IT security policies
  - Conducts review of DET IT security policies with enterprise applicability per Appendix B – DET IT Security Policy Process
- Division of Enterprise Technology - Bureau of Security
  - Creates policy review and approval procedures
  - Maintains the DET IT security policy and standards review schedule
  - Publishes updates to the DET Customer Portal as necessary

- Fields all customer requests for exceptions to DET IT security policies
- Provides IT security consulting support as it relates to regulatory requirements and best practice

COMPLIANCE

The DET IT security policies contained in this handbook shall take effect upon approval and publication. The DET Bureau of Security shall facilitate a review of the handbook at least once every year to ensure relevancy.

If compliance with the policies or related standards is not feasible or technically possible, or if deviation is necessary to support a business function, agency representatives shall request an exception through the DET Bureau of Security exception procedure.

COORDINATION AMONG AGENCIES

The State of Wisconsin Division of Enterprise Technology (DET) consolidated data center customer base is subject to multiple regulatory requirements designed to ensure the effective implementation of appropriate IT security measures. Listed below are some of the primary regulatory requirements.

- IRS Publication 1075
- HIPAA Security Rule #164, March 2013
- CJIS Security Policy – Version 5.3
- PCI Data Security Standard – Version 3.0
- FERPA Compliance

The DET consolidated data center shares responsibility with 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). DET employs mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries.

DET may designate selected controls as agency-defined. Implementation of some controls may need to be done in partnership between DET and the regulated agency; however the 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 4 which is used as the primary reference point by the DET Bureau of Security.

ENFORCEMENT/SANCTIONS

Any violation of the DET IT security policies stated herein is punishable by discipline, up to and including discharge. Violations of these policies which also constitute a criminal act shall be referred to law enforcement. All determinations regarding appropriate sanctions for violations of DET IT security policies will be made in consultation with the DOA Human Resources Department, in accordance with the State of Wisconsin's Disciplinary Action Policy.

IT SECURITY GOVERNANCE-Terminology & 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 the organization
  - ‘…protect valuable information, sensitive data, and the state computer infrastructure from unauthorized access, compromise, and corruption…”

- **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

- **Standards**
  - A mandatory action or rule 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 documents to align 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.

- DET IT security policies will be presented to State CIO for review and approval
- Enterprise-related IT security policies and standards will be presented to Agency CIO Steering Committee (ACSC) for review, approval, and oversight
- IT Security guiding principles, policies, standards, and procedures will be issued by the DET and have an assigned owner depending on the applicable security function

Communication

- All approved guiding principles, policies, and standards will be published to the DET Customer Portal, Enterprise IT page.
- Policies and procedures will be communicated to all appropriate personnel (Enterprise or DET) via email upon policy approval
- Policies will also be incorporated into the State of Wisconsin IT Security Awareness Training Program

Sustain

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

- DET IT security policies and standards will be reviewed on an annual basis at a minimum
- DET Bureau of Security personnel will:
    - Create policy review and approval procedures
    - Maintain the policy review schedule
    - Publish DET IT security guiding principles, policies, and standards to the DET Security Portal
    - Maintain a single repository for documentation
    - Coordinate the review of exception requests to DET IT security policies and standards

IT SECURITY POLICIES

AC-01 Access Control Policy

- Purpose
  - This policy establishes the Access Control Policy, for managing 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 and procedures 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 '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).
- Links to standards

AC-2	Account Management
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-6	Least Privilege
AC-7	Unsuccessful Logon Attempts
AC-8	System Use Notification
AC-11	Session 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 Information Systems
AC-21	Information Sharing
AC-22	Publicly Accessible Content

- Compliance References
  - CJISD 08140, Policy Area 5.1 Access Control
  - HIPAA 45 CFR 164.308, 164.312
  - IRS 1075, 9.3.1.1 Access Control
  - NIST 800-53 Revision 4, AC-01 Access Control Policy

AT-01 Security Awareness and Training

- Purpose
  - This policy establishes the Security Awareness and Training Policy, 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, and DET IT security policies.

- Policy
  - DET will develop and/or procure, and make available online security awareness training with a focus on DET IT security policies, security best practices; role based security and responsibilities for all agency personnel, contractors and interns to ensure that understanding of DET IT security policies and current IT security best practices. It is a requirement that all DET employees, contractors and interns receive security awareness and disclosure training upon employment and complete the online refresher security awareness training annually.
- Links to standards
  - AT-2 Security Awareness Training
  - AT-3 Role-Based Security Training
  - AT-4 Security Training Records
- Compliance References
  - IRS 1075, 9.3.2.12 Security Awareness
  - IRS 6103 (p)(4)(D);6.1
  - NIST 800-53 Revision 4, AT-01

AU-01 Audit and Accountability

- Purpose
  - This policy establishes the Audit and Accountability Policy, for managing risks from inadequate event logging and transaction monitoring. The related audit and accountability standards and procedures ensure the implementation security best practices with regard to event logging and transaction monitoring and the retention of audit evidence.
- Policy
  - Audit and log functions 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 user name/ID. Event storage retention must remain in compliance with regulatory requirements and be supported with an appropriate amount of disk storage for the required retention period. Time-stamps capabilities shall be synchronized for monitoring auditable devices and events.
- Links to standards
  - AU-2 Audit Events
  - AU-3 Content of Audit Records
  - AU-4 Audit Storage Capacity
  - AU-5 Response to Audit Processing Failures
  - AU-6 Audit Review, Analysis, and Reporting
  - AU-7 Audit Reduction and Report Generation
  - AU-8 Time Stamps
  - AU-9 Protection of Audit Information
  - AU-11 Audit Record Retention
  - AU-12 Audit Generation
  - AU-16 Cross-Agency Auditing

- Compliance References
  - IRS 1075, 9.3.3.1 Audit and Accountability
  - NIST 800-53 Version 4, AU-01

CA-01 Security Assessment and Authorization

- Purpose
  - This policy establishes the Security Assessment and Authorization Policy, for managing risks from inadequate security assessments, authorization, and continuous monitoring of agency information assets through the establishment of an effective security assessment program and procedures to facilitate this policy. The security planning program and associated procedures helps to implement security best practices with regard to security assessments, authorization, and continuous monitoring.
- Policy
  - Security assessments must be conducted on an annual basis to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established regulatory requirements. Security assessment reports must be formally documented and reported to DET IT Senior Leadership, 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.
- Links to standards
  - CA-2 Security Assessments
  - CA-3 System Interconnections
  - CA-6 Security Authorization
  - CA-7 Continuous Monitoring
- Compliance References
  - IRS 1075, 9,3,4,1 Assessment and Authorization
  - NIST 800-53 Version 4, CA-01
  - PCI DSS Version 2.0 Sections 12.1.1 and 12.1.2

CM-01 Configuration Management

- Purpose
  - This policy establishes the Configuration Management Policy, for managing risks from system changes impacting baseline configuration settings, system configuration and security based on the principle of ‘least function’. The configuration management procedures will help document, authorize, manage and control system changes impacting information system components within the control of DET Bureau of Infrastructure Support.
- Policy
  - To ensure a ‘secured’ and consistent implementation of protection mechanisms, baseline configurations and supporting procedures for each of the DET Infrastructure components must be developed, documented and maintained. These baselines derived from the USGCB and regulatory requirements shall be reviewed and updated based on changes to the infrastructure landscape by the DET Bureau of Infrastructure Support throughout the component life cycle, including destruction or disposal.
- Links to standards
  - CM-2 Baseline Configuration

  - CM-3 Configuration Change Control
  - CM-6 Configuration Settings
  - CM-7 Least Functionality
  - CM-8 Information System Component Inventory
  - CM-10 Software Usage Restrictions
- Compliance References
  - IRS 1075, 9.3.5.1 Configuration Management
  - NIST 800-53 Version 4, CM-01
  - PCI DSS Version 2.0, Section 1.1.2

CP-01 Contingency Planning

- Purpose
  - To ensure continuation of operations, this policy establishes the Contingency Planning Policy, 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 with regard to enterprise business continuity and disaster recovery.
- Policy
  - All essential mission critical DET infrastructure components (hardware and software) will be identified, documented within a formal contingency planning procedures which defines recovery objectives, restoration priorities, success metrics that include defined recovery time and recovery point objectives, roles and responsibilities, and contact lists. The contingency plan must be tested on an annual basis to include alternate site storage and processing, and mission critical components, or as requested by the agencies of the State of Wisconsin.
- Links to standards
  - CP-2 Contingency Plan
  - CP-3 Contingency Training
  - CP-4 Contingency Plan Testing
  - CP-6 Alternate Storage Site
- Compliance References
  - HIPAA 45CFR 164.310(a)(2)(i)
  - IRS 1075, 9.3.6.1 Contingency Planning
  - NIST 800-53 Version 4, CP-01

IA-01 Identification and Authentication

- Purpose
  - This policy establishes the Identification and Authentication Policy, for managing risks from user access (organizational, non-organizational) and authentication into agency information assets through the establishment of an effective identification and authentication program. The identification and authentication procedure helps in implementing security best practices with regard to identification and authentication into DET managed information assets and required infrastructure components.
- Policy

  - Individuals attempting access to DET managed networks (internal or external) or enterprise systems must be uniquely identified and authenticated before the establishment of a connection to the State of Wisconsin DET managed networks.
- Links to standards
  - IA-2 Identification and Authentication (Organizational 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-Organizational Users)
- Compliance References
  - IRS 1075, 9.3.7.1 Identification and Authorization
  - NIST 800-53 Version 4, IA-01

IR-01 Incident Response

- Purpose
  - This policy is to establish guidelines for the identification, response, reporting, assessment, analysis, and follow-up to all suspected information security incidents. The related information security response procedure helps 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. DET shall develop formal Incident Response Procedures that include the areas of IT security incident event identification, notification, containment, eradication and recovery.
  - DET shall:
    - Train personnel, including contractors, in their incident response roles.
    - Test the incident response capability at least annually.
    - Require personnel to report suspected security incidents to DET Bureau of Security upon discovery of the incident
- Links to standards
  - IR-2 Incident Response Training
  - IR-3 Incident Response Testing
  - IR-4 Incident Handling
  - IR-5 Incident Monitoring
  - IR-6 Incident Reporting
- Compliance References
  - CJIS ITS 08140 Policy Area 5.1
  - HIPAA DSS Version 2, 45 CFR 164.308(a)(6)(i), 164.308(a)(6)(ii)
  - IRS 1075, 9.3.8.1 Incident Response
  - NIST 8001-53 Version 4, IR-01
  - PCI DSS Version 2, Sections 12.9.3, 12.9.4

MA-01 System Maintenance

- Purpose
    - This policy establishes the System Maintenance Policy, for managing risks associated with information asset maintenance and repairs through the establishment of an effective System Maintenance Procedures. The related system maintenance standards and procedures will ensure the implementation of security best practices with regard to enterprise system maintenance and repairs.
- Policy
    - Formal and documented procedures must be developed to ensure consistent practices in regard to the scheduling, performing, documenting, reviewing and recording of maintenance and repairs for all infrastructure components in accordance with manufacturer or vendor specifications, or specific DET published maintenance requirements.
    - Personnel performing maintenance on the information system components must have appropriate identification and/or been previously authorized by DET.
- Links to standards
    - MA-2 Controlled Maintenance
    - MA-3 Maintenance Tools
    - MA-4 Non-Local Maintenance
    - MA-5 Maintenance Personnel
- Compliance References
    - IRS 1075, 9.3.10.1 System Maintenance
    - NIST 800-53 Version 4, MA-01

MP-01 Media Protection

- Purpose
    - This policy establishes the Media Protection Policy, for managing risks from media access, media storage, media transport, and media protection through the establishment of effective Media Protection Procedures. The media protection procedures will ensure the implementation of security best practices and control activities with regard to enterprise 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 of 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.
- Links to standards
    - MP-2 Media Access
    - MP-4 Media Storage
    - MP-5 Media Transport
    - MP-6 Media Sanitization

- Compliance References
  - CJIS ITS 08140 Policy Area 5.1
  - IRS 1075, 9.3.10.1 System Maintenance
  - NIST 800-53 Version 4, MP-01
  - PCI DSS Version 2, Section 9.1

PE-01 Physical and Environmental Protection

- Purpose
  - This policy establishes the Physical and Environmental Protection Policy, for mitigating the risks from physical security and environmental threats through the establishment of an effective physical security and environmental control procedures. The physical security and environmental controls program helps protect its IT assets from physical and environmental threats whether internal or external.
- Policy
  - Physical access to DET infrastructure facilities where sensitive/confidential informational assets or infrastructure reside must be strictly limited to personnel requiring access to buildings or sensitive areas within the DET Infrastructure Facilities. For visitors, documentation must be retained to capture the individual identification by showing formal identification documentation-(re: driver's licenses, state or government ID's containing photo). All personnel granted access to restricted buildings must display appropriate identification badges above the waist. Identification badges shall be displayed above the waist at all times while remaining inside of the building.
  - Environmental control equipment (HVAC), monitoring systems and required power cabling, control boxes, or piping must be protected 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. These protection mechanisms must be employed at all required alternate work sites where sensitive/confidential information resides.
- Links to standards
  - PE-2 Physical Access Authorizations
  - PE-3 Physical Access Control
  - PE-6 Monitoring Physical Access
  - PE-8 Visitor Access Records
- Compliance References
  - HIPAA 45 CFR 164.310(a)(2)(ii)
  - IRS 1075, 9.3.11.1 Physical Environment
  - NIST 800-53 Version 4, PE-01
  - PCI DSS Version 2, Section 9.6

PL-01 Security Planning

- Purpose
  - This policy establishes the Security Planning Policy, for managing risks from inadequate security planning through the establishment of an effective security planning program. The related security planning procedures ensure the implementation of security best practices with regard to enterprise security planning, preparation, and strategy.

- Policy
  - An IT security plan will be developed to assure the protection of the State of Wisconsin information assets and supporting infrastructure by explicitly defining the authorization boundaries of the DET-supported systems and identifying information relationships and connections both external to the state's network and sensitive or regulated information in transit both inbound and outbound to the DET data center, and while at rest on DET storage technologies.
- Links to standards
  - PL-4 Rules of Behavior
- Compliance References
  - HIPAA 45 CFR 164.310(d)(2)(i)(i)(ii)
  - IRS 1075, 9.3.12.1 Security Planning
  - NIST 800-53 Version 4, PL-01
  - PCI DSS Version 2, Section 12.1.3

PS-01 Personnel Security

- Purpose
  - This policy establishes the Personnel Security Policy, for managing risks from personnel screening, termination, management and third-party (contractors, vendors, interns) access, through the establishment of an effective security planning procedures. The personnel security procedures ensure the implementation security best practices with regard to personnel screening, termination, transfer and management.
- Policy
  - Personnel seeking employment in the Division of Enterprise Technology are required to have personnel screening and/or background checks performed prior to employment.
  - Access to infrastructure components containing State of Wisconsin information by third-party vendors or contractors is also subject to the same personnel security requirements. The personnel security requirements for each type of role must be formally documented and monitored for individual compliance. Third-party vendors or contractors are also subject to established DET IT security policies. Access agreements between the State of Wisconsin DET and vendor/contractors must be reviewed and updated on an annual basis.
- Links to standards
  - PS-2 Position Risk Designation
  - PS-3 Personnel Screening
  - PS-4 Termination
  - PS-6 Access Agreements
- Compliance References
  - IRS 1075, 9.3.13.1 Personnel Security
  - NIST 800-53 Version 4, PS-01
  - CJIS ITS 08140 Policy Area 5.12

RA-01 Risk Assessment

- Purpose
    - This policy establishes the Risk Assessment Policy, for managing risk from vulnerabilities, determining areas of vulnerabilities, initiating appropriate remediation activities by the Bureau of Infrastructure Support and the establishment of effective risk assessment methodology and procedures. The related Risk Assessment Procedures will ensure the implementation of security best practices with regard to identifying known vulnerabilities to DET managed infrastructure components supported by Bureau of Infrastructure Support.
- Policy
    - Timely risk assessments of the DET managed infrastructure are required to protect against potential threats and vulnerabilities to the states information system infrastructure from being compromised in the areas of confidentiality, integrity, and availability of sensitive and confidential information.
- Links to standards
    - RA-3 Risk Assessment
    - RA-5 Vulnerability Scanning
- Compliance References
    - IRS 1075, 9.3.14.1 Risk Assessment
    - NIST 800-53 Version 4, RA-01

SA-01 System and Services Acquisition

- Purpose
    - This policy establishes the System and Services Acquisition Policy, for managing risks from third party products and services' providers, through the establishment of an effective third party risk management procedures. The related third party risk assessment procedure helps ensures the implementation of security best practices with regard to the acquisition of Systems and Services from third-party providers.
- Policy
    - The acquisition of systems and services are subject to a formal security assessment review to include 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.
- Links to standards
    - SA-3 System Development Life Cycle
    - SA-8 Security Engineering Principles
    - SA-9 External Information System Services
- Compliance References
    - IRS 1075, 9.3.13.1 System and Services Acquisition
    - NIST 800-53 Version 4, SA-01

SC-01 System and Communication Protection

- Purpose
  - This policy establishes the System and Communications Protection Policy, for managing risks from vulnerable system configurations, denial of service, data communication and transfer. The associated system and communications protection procedures help implement security best practices with regard to system configuration, data communication and transfer as it relates to the availability, confidentiality or integrity of information.
- Policy
  - Sensitive and confidential information, whether at rest or in-transit must be protected from accidental or intentional threats that could corrupt, modify, delete or disclose information in the DET consolidated data center. Controls must consider threats from denial of service, attacks against network boundaries, during transmission, network disconnects, collaborative computing devices, other critical infrastructure components, multi-function devices and printers.
- Links to standards
  - SC-7 Boundary Protection
  - SC-8 Transmission Confidentiality and Integrity
  - SC-10 Network Disconnect
  - SC-12 Cryptographic Key Establishment and Management
  - SC-13 Cryptographic Protection
  - SC-15 Collaborative Computing Devices
  - SC-17 Public Key Infrastructure Certificates
  - SC-23 Session Authenticity
  - SC-28 Protection of Information at Rest
- Compliance References
  - HIPAA 45 CFR 164.308 (a)(1)(i), 164.308(a)(3)(ii)
  - IRS 1075, 9.3.16.1 System and Communication Protection
  - NIST 800-53 Version 4, SC-01

SI-01 System and Information Integrity

- Purpose
  - This policy establishes the System and Information Integrity Policy, for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an effective System and Information Integrity program. The related system and information integrity procedures help DET implement security best practices with regard to system configuration, security, and error handling.
- Policy
  - Business Systems must:
    - Identify, report, and correct information system flaws.

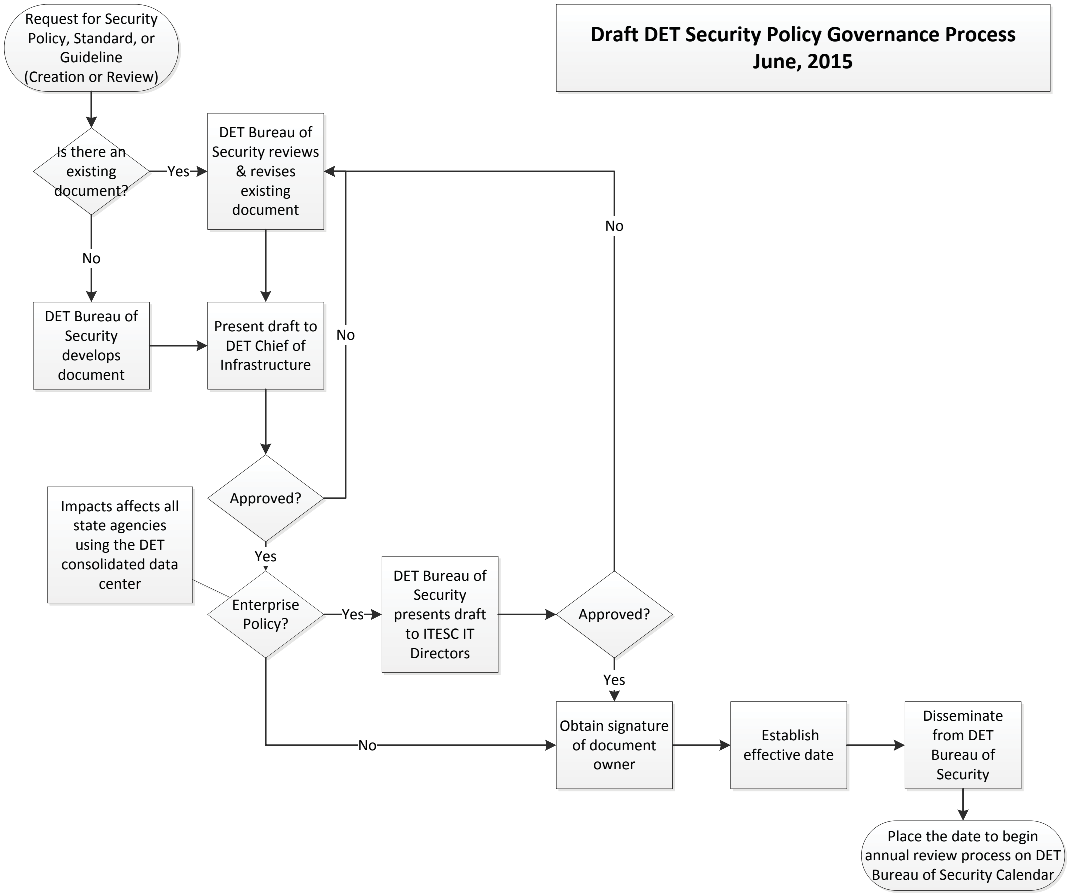
        - Test software updates related to flaw remediation for effectiveness and potential side effects on organizational information assets before installation.
        - Incorporate flaw remediation into the organizational configuration management process.
        - Employ, configure and update malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices (e.g., email, removable media, and malicious websites) 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 infrastructure security event mechanisms must have event detection monitoring, capturing and reporting of violation events. Violation event records are required to be logged and retained based on current regulatory requirements (currently seven years).
- Links to standards
    - SI-2 Flaw Remediation
    - SI-3 Malicious Code Protection
    - SI-4 Information System Monitoring
    - SI-8 Spam Protection
    - SI-11 Error Handling
- Compliance References
    - IRS 1075, 9.3.17.1 System and Information Integrity
    - NIST 800-53 Version 4, SI-01

APPENDICES

Appendix A - ACRONYMS

CISO	Chief Information Security Officer
CJIS	Criminal Justice Information Services
DET	Department of Administration – Division of Enterprise Technology
DOA	Department of Administration
FERPA	Family Educational Rights and Privacy Act
HIPAA	Health Insurance Portability and Accountability Act
IRS	Internal Revenue Service
ITGC	Information Technology General Controls
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard

Appendix B - DET IT Security Policy Governance Process


Draft DET Security Policy Governance Process
June, 2015
Request for Security Policy, Standard, or Guideline (Creation or Review)
Is there an existing document?
Yes
No
DET Bureau of Security reviews & revises existing document
DET Bureau of Security develops document
Present draft to DET Chief of Infrastructure
No
Approved?
Yes
Impacts affects all state agencies using the DET consolidated data center
Enterprise Policy?
Yes
DET Bureau of Security presents draft to ITESC IT Directors
Approved?
No
Yes
No
Obtain signature of document owner
Establish effective date
Disseminate from DET Bureau of Security
Place the date to begin annual review process on DET Bureau of Security Calendar

Appendix C - Glossary/Definitions

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.

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 facilitate the continuity of operations in an emergency situation.

Control An action taken to enhance the likelihood that established goals or objectives will be achieved (in the context of this policy, generally an action taken to reduce risk.)

Data A subset of information in an electronic format that allows it to be retrieved or transmitted

Identification The process that enables recognition verification of a user

Incident A computer security incident is defined by NIST as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. A computer security incident is also defined as any event that adversely affects the confidentiality, integrity, or availability of system and its data.

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 representation of facts, concepts or instructions created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media. This may include, but is not limited to the data contained in reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

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 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 an IT against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of ITs and data. IT security includes consideration of all hardware and/or software functions

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 D - Review, Revision, Approval Log

Version #	Revision or Review Date	Description of Changes	Author-Title
0.1	06/12/15	Initial draft version circulated for review	Jeff Thompson - Compliance
0.2	06/16/16	Draft approved for governance review	Jeff Thompson - Compliance
0.3	08/31/15	Updated after comments from agencies	Jeff Thompson - Compliance

Approved by:

___________________________________ Date: _______________________
CIO, Division of Enterprise Technology