POLICY 1340.00 Information Technology Information Security

Issued: April 12, 2007
Revised: May 27, 2025
Reviewed: October 31, 2024
Next Review Date: May 27, 2026

APPLICATION

This policy is for statewide compliance and is applicable to all information systems that are part of the Executive Branch Departments, Agencies, Boards or Commissions, and business or vendor partners that manage state of Michigan (SOM) information technology (IT) resources including, but not limited to, networks, systems, computers, data, databases, and applications.

The DTMB Deputy Director of Cybersecurity & Infrastructure Protection (CIP) as the Chief Security Officer (CSO) shall enforce SOM IT security standards with authority under MCL 18.1101, et seq; MCL 18.41; Executive Order 2001-3; and Executive Order 2009-55. CIP is accountable to the DTMB Chief Information Officer (CIO) for identifying, managing, and mitigating physical and IT security risks and vulnerabilities within SOM facilities and computing, communication, and technology resources. CIP also oversees physical and IT security risk management, awareness, and training; assists SOM agencies with their security issues; and enforces oversight of SOM security PSPs to maintain suitable levels of enterprise-wide security as assisted by Agency Security Officers (ASO).

To secure the enterprise IT environment, CIP has selected the Risk Management Framework published by the National Institute of Standards and Technology (NIST) current revision, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (nist.gov) and tailored controls from NIST Special Publication 800-53 current revision, Security and Privacy Controls for Information Systems and Organizations (nist.gov) from the NIST Computer Security Resource Center. Each System Security Plan (SSP) will address NIST security standards and guidelines including any additional controls if required in the following policies and corresponding standards and procedures as well as Agency specific regulatory requirements as may apply to that Agency.

PURPOSE

CIP is committed to securing SOM assets and provides the NIST security framework for developing, implementing, and enforcing security Policies, Standards, and Procedures (PSPs) to prevent or limit the effect of a failure, interruption, or security breach of the SOM's facilities and systems. This policy establishes the SOM strategic view of IT security for information systems that process, store, and transmit SOM information. Those who implement and manage information systems must address security controls applicable to corresponding systems as identified in this policy and corresponding standards and procedures.

CONTACT AGENCY

Department of Technology, Management and Budget (DTMB)
Cybersecurity & Infrastructure Protection (CIP)

Telephone: 517-241-4090

SUMMARY

Security controls must be implemented to protect SOM information from unauthorized access, use, disclosure, modification, destruction, or denial and to ensure confidentiality, integrity, and availability of SOM information. All SOM employees, trusted partners, or entities authorized to access, store, or transmit SOM information shall protect the confidentiality, integrity, and availability of the information as set forth in this and all SOM enterprise IT Policies, Standards, and Procedures (PSPs). Information is not limited to data in computer systems and is included wherever it resides in an agency, whatever form it takes, (electronic, printed, etc.), whatever technology is used to handle it, or whatever purposes it serves. Any data that is originated, entered, processed, transmitted, stored, or disposed of for the SOM is considered SOM information and is also recognized as "state data."

PSPs addressed in this document and corresponding sub-level documents include management, operational, and technical controls. The corresponding standards and procedures are available to SOM employees at: The Bridge Policies - IT Policies, Standards and Procedures.

SOM or environmental changes may require changes to this security policy. Any efforts to request, approve, implement, or communicate changes to PSPs that this policy regulates or governs must be made under SOM 1305.00.01 IT Policy Administration Standard.

Policy exceptions could occur for many reasons. Examples include an overriding business need, a delay in vendor deliverables, new regulatory or statutory requirements, and temporary configuration issues. The exception process must ensure these circumstances are addressed while making all stakeholders aware of the event, risks, and timetable to eliminate the exception. If an exception to this policy or a related standard is necessary, agencies, in conjunction with their DTMB representatives, must comply with the approved DTMB process outlined in the SOM 1305.00.02 Technical Policy and Product Exception Standard and the SOM 1305.00.02.01 Technical Review Board (TRB) and Executive Technical Review Board (ETRB) Exception Procedure.

CIP will duly implement and enforce security PSPs to ensure their effective dissemination and availability. CIP may enforce compliance through continuous monitoring, security accreditation process, vulnerability scanning, and other validation methods to ensure an adequate level of security is maintained. ASOs are obligated to assist CIP with these implementation and enforcement efforts.

General

The following SOM standards are established in accordance with corresponding NIST controls. This policy establishes these standards and related standards and procedures to effectively implement corresponding SOM Cyber Security baseline controls on the identified subjects. All SOM Agencies must develop, adopt, and adhere to a formal, documented process that addresses purpose, scope, roles, responsibilities, management commitment, coordination among SOM entities, and demonstrates compliance with each of the following standard areas. Each PSP must be reviewed annually and updated as needed.

The risk management strategy is an important factor in establishing such PSPs. PSPs contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of SOM PSPs. The policy can be included as part of the general security and privacy PSPs or be represented by multiple PSPs reflecting the complex nature of Agencies. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the PSPs or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to PSPs include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

020 Access Control Standard[1]

Access control standard and procedures address the controls in the AC Family that are implemented within systems and organizations.

030 Awareness and Training Standard[2]

Awareness and training standard and procedures address the controls in the AT Family that are implemented within systems and organizations.

040 Audit and Accountability Standard[3]

Audit and accountability standard and procedures address the controls in the AU Family that are implemented within systems and organizations.

---

[1] AC-01; L/M/H;
[2] AT-01; L/M/H;
[3] AU-01; L/M/H;

050 Assessment, Authorization, and Monitoring Standard[4]

Assessment, authorization, and monitoring standard and procedures address the controls in the CA Family that are implemented within systems and organizations.

060 Configuration Management Standard[5]

Configuration management standard and procedures address the controls in the CM Family that are implemented within systems and organizations.

070 Contingency Planning Standard[6]

Contingency planning standard and procedures address the controls in the CP Family that are implemented within systems and organizations.

080 Identification and Authentication Standard[7]

Identification and authentication standard and procedures address the controls in the IA Family that are implemented within systems and organizations.

090 Incident Response Standard[8]

Incident response standard and procedures address the controls in the IR Family that are implemented within systems and organizations.

100 Maintenance Standard[9]

Maintenance standard and procedures address the controls in the MA Family that are implemented within systems and organizations.

110 Media Protection Standard[10]

Media protection standard and procedures address the controls in the MP Family that are implemented within systems and organizations.

120 Physical and Environmental Protection Standard[11]

Physical and environmental protection standard and procedures address the controls in the PE Family that are implemented within systems and organizations.

---

[4] CA-01; L/M/H;
[5] CM-01; L/M/H;
[6] CP-01; L/M/H;
[7] IA-01; L/M/H;
[8] IR-01; L/M/H;
[9] MA-01; L/M/H;
[10] MP-01; L/M/H;
[11] PE-01; L/M/H;

130 Planning Standard[12]

Planning standard and procedures address the controls in the PL Family implemented within systems and organizations.

140 Personnel Security Standard[13]

Personnel security standard and procedures address the controls in the PS Family that are implemented within systems and organizations.

150 Risk Assessment Standard[14]

Risk assessment standard and procedures address the controls in the RA Family that are implemented within systems and organizations.

160 System and Services Acquisition Standard[15]

System and services acquisition standard and procedures address the controls in the SA Family that are implemented within systems and organizations.

170 System and Communications Protection Standard[16]

System and communications protection standard and procedures address the controls in the SC Family that are implemented within systems and organizations.

180 System and Information Integrity Standard[17]

System and information integrity standard and procedures address the controls in the SI Family that are implemented within systems and organizations.

200 Program Management Standard[18]

An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

A formal standard will be created for this control family soon.

210 Personal Identifying Information Processing and Transparency Standard[19]

Personal Identifying Information (PII) processing and transparency standard and procedures address the controls in the PT Family that are implemented within systems and organizations.

---

[12] PL-01; L/M/H;
[13] PS-01; L/M/H;
[14] RA-01; L/M/H;
[15] SA-01; L/M/H;
[16] SC-01; L/M/H;
[17] SI-01; L/M/H;
[18] PM-01; L/M/H;
[19] PT-01; L/M/H;

A formal standard will be created for this control family soon.

220 Supply Chain Risk Management Standard[20]

Supply chain risk management standard and procedures address the controls in the SR Family as well as supply chain-related controls in other families that are implemented within systems and organizations.

A formal standard will be created for this control family soon.

ROLES AND RESPONSIBILITIES

The definitions of the Roles and Responsibilities are written to provide guidance and are not all inclusive. There may be additional duties that are required for the Roles listed below based on the individual Agency and applicable state and/or federal laws, rules, and regulations.

Agency

Agency Director:

- Ensures proper levels of protection for their Agency information are determined and documented, and necessary safeguards are implemented in accordance with SOM 1340.00.150.02 Data Classification Standard.
  - Data management complies with applicable state and/or federal laws, rules, regulations, and SOM policies.
  - Information security controls are implemented to protect SOM information, and sufficiently to ensure the confidentiality, integrity, and availability of SOM information.
- Ensures Business Owner is properly identified and classifying data.
- Ensures anyone requiring access to confidential or restricted information owned by another Agency obtains permission from the Business Owner.
- Ensures a formalized process is developed to manage user access to the SOM Network and IT resources in compliance with this and all SOM PSPs.
- Ensures a process is established to review technical controls and recommendations identified by SOM Data Custodians.
- Ensures Agencies follow DTMB policy on the system security planning process including SSPs.
- Ensures internal Agency security PSPs, that compliment and comply with this policy, are implemented, maintained, and enforced.

[20] SR-01; L/M/H;

- Ensures Agency employees and Trusted Partners handle information for which they are responsible in compliance with this policy and all applicable SOM PSPs.
- Ensures all Agency employees are trained to handle information in accordance with this and all SOM PSPs.
- Establishes an overall strategy for the Agency's Role-Based Security Program.
- Ensures that high priority is given within the Agency to implement effective security awareness and role-based security training for employees to protect state assets.
- Ensures SOM employees and Trusted Partners are trained to ensure awareness of their role in protecting SOM information and data as set forth in this policy.
- Ensures employees are advised of the necessity of complying with SOM policies and laws on the protection of SOM information, because non-compliance may leave the SOM and employees subject to prosecution, civil suits, and disciplinary action.
- May implement more stringent PSPs than those developed by DTMB for the SOM in conjunction with DTMB.

Agency Authorizing Official (Delegated Authority)

- Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

Agency Security Officer (ASO)

- An Agency official with operational authority for securing agency information and establishing controls for its generation, collection, processing, dissemination, and disposal.
- Assists the Agency Information System Owners (ISOs) and Information Owners (IOs) in ensuring that information systems have adequate security controls in place to meet all applicable state and/or federal laws, rules, and regulations.
- Administers an Agency information security program or serve as the Security Control Assessor.
- Serves as primary liaison between the Agency and DTMB, Data Custodians, Common Control Providers, and External Service Providers.
- Responsible for maintaining the security posture for their Agency information systems or programs.
- Assists in the development and compliance of security PSPs and classifying information assets.

- Assists the IO and ISO in completing the SSP and Plan of Action and Milestone (POAM).
- Reviews and responds to security notifications from the Michigan Security Operations Center (MiSOC).
- Serves as a principal advisor on all matters, technical and otherwise, involving the security of Agency's information and information systems.
- Oversees the protection of information through physical and environmental protection, personnel security, incident handling, and security awareness within the Agency.
- Ensures implementation of security awareness training within the Agency.
- Works with the statewide security awareness training coordinator to implement statewide general security awareness training programs within the Agency.
- Ensures that appropriate role-based training materials are timely developed and executed for intended Agency audiences.
- Assists Agency managers in establishing a tracking and reporting strategy for security training.
- Coordinates with Agency personnel (i.e. ISO and designees, Office Directors, DTMB - Agency services (DTMB-AS), data custodians, and others as designated) for maintaining the confidentiality, integrity, and availability of information and information systems.

Agency Privacy Officer

- Ensures that the Agency's collection, processing, dissemination, and disposal of data complies with the state and federal privacy laws and regulations.
- May assist the ISO and IO in completing the SSP and POAM.
- This role may be the same as ASO depending on the Agency.

Business Owner

- May own information or information systems that support the primary business functions served by the application and is the application's largest stakeholder.
- Supports the business function by making decisions for all owners of the data.
- Administers systems and may delegate to the System Administrators.
- Typically, the Business Owner is also an ISO.

Information System Owner (ISO)

- The ISO has the following responsibilities for SSPs:

- Develops the SSP in compliance with the 1340.00 Security Standards, in collaboration DTMB - Agency Services and Michigan Cyber Security (MCS) Security Liaisons, and functional end users.
- Categorizes the information system based on Federal Information Processing Standards (FIPS) 199, NIST SP 800-60, SOM 1340.00.150.02 Data Classification Standard, and other standards encompassed by this policy.
- Maintains the SSP and ensures that the system is deployed and operated according to agreed-upon security requirements.
- Decides who has access to the system and the types of privileges and access rights.
- Ensures that system users and support personnel receive required security training.
- Updates the SSP when a significant change occurs.
- Assists in identifying, implementing, and assessing the common security controls.

- Responsible for the POAM process in collaboration with the ASO, DTMB - Agency Services, Michigan Cyber Security (MCS) Security Liaisons, and functional end users.
- Informs appropriate Agency and DTMB officials of the need to conduct the security authorization, ensures necessary resources are available and provides the required information system access, information, and documentation. This is usually a collaborative effort with Agency Services and the ASO.
- Coordinates with CIP on assembling and submitting the authorization package to the Authorizing Officials identified in the SSP.
- Permits and documents information from multiple IOs, if applicable.

Information Owner (IO)

- Establishes the rules for appropriate use and protection of the subject data or information.
- In coordination with the ISO, categorizes the information system based on FIPS 199, NIST SP 800-60, SOM 1340.00.150.02 Data Classification Standard and other standards encompassed by this policy.
- Provides input to ISOs on the security requirements and security controls for the information system where the information resides.
- Assists in identifying and assessing the common security controls where information resides.
- Decides who can access the information system and the types of privileges and access rights.

- Establishes the rules for behavior for appropriate use and protection of the information and retains that responsibility when the information is shared with or provided to other organizations.

Managers and Supervisors

- Support their unit and respective Agency's mission and business functions.
- Serve in the role of ISO and IO, if applicable.
- As authorized by the IO, may handle the day-to-day security operations of a system.
- Consider developing Individual Development Plans (IDPs) for employees with security responsibilities.
- Promote the professional development and certification of IT security program employees and others with significant security responsibilities.
- Ensure that all employees are appropriately trained in how to fulfil their security responsibilities before allowing access to Agency information systems.
- Ensure that employees understand specific rules of each system and application they use.
- Work to reduce errors and omissions by users due to lack of awareness and training.
- Comply with IT security awareness and training requirements established for their users.
- Work with their Agency Security Awareness Training Coordinator to meet shared responsibilities.

Security Administrator Responsibilities for Users

- Responsible for all security attributes of a user or role and for the following tasks:
    - Assigning and modifying the security attributes of a user, role, or rights profile (read, write, execute, etc.).
    - Creating and modifying rights profiles.
    - Assigning rights profiles to a user or role.
    - Assigning privileges and authorizations to a user, role, or rights profile.
    - Removing privileges or authorizations from a user, role, or rights profile.
- Typically, the Security Administrator role creates rights profiles. However, if a profile needs capabilities that the Security Administrator role cannot grant, then superuser or the Primary Administrator role can create the profile.

Security Control Assessor

- The individual, group, or Agency responsible for conducting a security control assessment.

Users

- Includes all state employees, contractors; guests, visitors, other collaborators, and associates requiring access to SOM data or resources working in staff augmentation positions; students; or Trusted Partners.
- Understand and comply with federal, statewide and Agency IT/cybersecurity policies and procedures.
- Are trained in the rules of behavior for the systems and applications to which they have access.
- Work with management to meet training needs.
- Keep software and applications updated with security patches on their assigned device.
- Are aware of actions they can take to better protect SOM information, including:
    - Proper password usage.
    - Using proper antivirus protection.
    - Reporting any suspected incidents or violations of security policy.
    - Following rules established to avoid social engineering attacks.

Information Technology (IT) Roles

Common Control Provider

- Responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls or privacy controls inherited by information systems).
- Documents organization-identified common controls in a SSP, ensuring that a security risk assessment is performed by appropriate personnel and a POAM is produced.
- Informs Risk and Compliance Division (RCD) when problems arise in inherited common controls.
- Maintains compliance of their common controls with applicable federal, state, and regulatory frameworks' security controls to benefit all systems inheriting the common controls.
- Typically, DTMB provides inheritable controls as a centralized IT service provider, however individual agencies may also provide enterprise services.

DTMB Chief Information Officer (CIO)

- Directs the strategic design, acquisition, management, and implementation of the statewide technology infrastructure.
- Consistent with the Federal Information Security Modernization Act (FISMA), administers training and oversees personnel with significant IT/cybersecurity responsibilities.
- Ensures a statewide IT/cybersecurity program is implemented.
- Ensures resources and budgets are available to support the IT/cybersecurity program.
- Measures effectiveness of the IT/cybersecurity program.
- Designates a Chief Technology Officer (CTO) to manage information systems and assets for Enterprise Architecture, Service Providers, Infrastructure and Operations, Network Strategies, and Research and Technology Implementation.
- Designates a CSO to develop and maintain a statewide CIP program to fulfill the Director's responsibilities for system security planning.
- Ensures that Agency Directors, Agency Authorized Officials, ISOs, IOs, Data Custodians, and other related personnel understand the concepts and strategy of the IT/cybersecurity program.
- Ensures that Agencies have access to SOM PSPs, and guidelines governing user access to the SOM network and IT Resources.
- Ensures a formal process is established to manage user access to the SOM network and IT Resources (local area network (LAN), wide area network (WAN), file and print, desktop, etc.).
- Ensures a formal process is established to implement and audit Agency-approved access requests to established services, (wireless, Telecom catalog services, application access, new employee access, etc.) on the SOM network in compliance with this and all SOM PSPs.
- Ensures a formal process is established that ensures the proper implementation and integration of service continuity with other system operations and technical security controls as required by DTMB in conjunction with Agencies.
- Ensures Agency-required security controls and safeguards are implemented and monitored for compliance.
- Ensures that all System End Users of information systems are sufficiently trained in their security responsibilities.

DTMB Chief Technology Officer (CTO)

- Determines the strategic direction of SOM technology function.

- Maintains technology policies and standards on Enterprise IT, IT Network and Infrastructure, and Configuration Management.
- Directs the activities necessary to keep the technology infrastructure efficient and effective while ensuring compliance with established PSPs.
- Manages information systems implementation and monitors effectiveness.
- Maintains information systems security and maintenance.
- Manages staff in functional areas such as LAN/WAN architecture, systems operations, and hardware support.
- Anticipates and reacts to major technology changes.
- Collaborates with the executive team to assess and recommend technologies in support of SOM needs.

DTMB Chief Security Officer (CSO)

- Establishes an enterprise information security program that includes planning, oversight, and coordination of its information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal activity, fraud, waste, and abuse in the use of information assets.
- Establishes and creates an overall strategy for a Statewide General Security Awareness Program available to all SOM Agency employees.
- Ensures that the Statewide General Security Awareness Program is funded.
- Ensures that SOM senior managers and others understand the concepts and strategy of the Statewide General Security Awareness Program and are informed of the progress of the program's implementation.
- Appoints a Statewide Security Awareness Coordinator to develop and implement the SOM Information Security and Privacy Awareness program.
- Develops and maintains information security PSPs and control techniques to address system security planning.
- Manages identification, implementation, and assessment of common security controls.
- Coordinates the development, review, and acceptance of SSPs with ISOs.
- Ensures that personnel with responsibilities for SSPs are trained.
- Ensures the policies defined in the Cyber Security Program align with the enterprise information security program.
- Develops and maintains data classification PSPs, and control techniques to protect SOM data from security incident or data breach.
- Establishes a governance body to direct the development of SOM enterprise entity-specific information security plans, PSPs, and other authoritative documents.

- Oversees the creation, maintenance, and enforcement of established enterprise information security PSPs, and guidelines.
- Develops and tracks information security and privacy risk key performance indicators.
- Develops and disseminates security and privacy metrics and risk information to SOM entity executives and other managers for decision making purposes.
- Coordinates security efforts with SOM entities and other branches of government as applicable.
- Establishes an access control program for state-owned and/or leased facilities, DTMB-managed facilities that includes planning, oversight, and coordination of program activities to effectively manage risk and provide a secure environment for employees and visitors.
- Provides monitoring of safety, security and building systems in DTMB-managed facilities and initiates emergency response as needed.
- Develops and maintains PSPs to address facility security planning and manages the identification, implementation, and assessment of common security controls.
- Reviews Security Authorization Packages and authorizes implementation of the information system.
- Responsible for identification and implementation of security protection and monitoring for all SOM IT networks.
- Ensures monitoring for improper storage of sensitive data on file/print shares, network attached file stores, and cloud solutions when applicable.
- Responsible for maintaining enterprise security posture.

DTMB Business Relationship Manager (BRM)

- Responsible for oversight and direction for both development and maintenance activities to keep the client agency's systems (i.e. DTMB and/or vendor solutions) operational and reliable, maintaining quick and accurate responses, as well as maintaining a highly competent and technical support staff.
- Serves as primary IT contact point with client agency and vendors communicating information concerning IT services and products.
- Carries out all division administrative duties in accordance with the agency's Service Level Agreement (SLA) and business plans.
- Ensures that the appropriate operational security posture is maintained for an information system working closely with the ASOs, ISOs, and IOs.
- Coordinates and conducts the required day-to-day technological management.

- In collaboration with the ISO, determine the technological planning and resourcing of the SSP and POAM.
- Has the detailed knowledge and expertise required to manage the security aspects of an information system of an Agency.

DTMB Data Custodian

- The primary point of contact between the MCS security liaison and data custodians/agency services in managing the completion of the SSP and Risk Assessment.
- A technical lead, who either knows the majority of system functionality and/or knows how to obtain the information.
- An individual, team, or Agency delegated by an ISO that has operational responsibility for technological management of information systems and data.
- Implements and manages the necessary safeguards to protect data based on requirements established by the ISO and documented in the SSP.
- Protects the information from unauthorized access.
- Provides IT support functions for Agencies.
- Assists BRMs and client Agencies to complete SSP.

Incident Manager

- Leads the IT team in promptly addressing and resolving any disruptions that arise within organizational technical infrastructure, this involves establishing clear protocols for incident detection, response, and resolution.

IT Service Provider

- An entity including DTMB and/or vendors who support and provide IT services.

MCS Security Liaison

- Technical and business security resource for the development, research, evaluation, recommendation, and planning of security controls and architecture for assigned agencies utilizing Governance Risk and Compliance (GRC) system.
- Identifies, coordinates and facilitates completion of the SSPs, Risk Assessments, and POAMs for an Agency.
- Works closely with the MCS Security Architects, ISOs, IOs, ASOs, Common Control Providers, and Data Custodians on security-related issues and services.
- Provides consistent communication, enhances security culture, and integrates governance, risk management, and compliance to reduce risk across SOM.

MCS Security Architect

- Ensures that information system security requirements necessary to protect the Agency's core missions and business processes are adequately addressed in all aspects of enterprise architecture.
- Identifies information security requirements necessary to protect the information system and ensures these requirements are adequately addressed in the SSP.
- Assists in providing a wide range of security-related services including:
  - Establishing information system boundaries.
  - Assessing the severity of weaknesses and deficiencies.
  - Supporting development and maintenance of PSPs.
  - Providing support for understanding security alerts and notifications.
  - Identifying potential adverse effects of identified vulnerabilities.
  - Supporting MCS objectives on enterprise teams and committees.

Statewide Security Awareness Training Coordinator

- Oversees the Statewide General Security Awareness Training Program, providing effective awareness and training materials which are periodically reviewed and updated, in part based on feedback from the intended audiences.

System Administrators

- Responsible for the installation and maintenance of an information system, providing effective information system utilization, incorporates secure configuration settings for IT products, adequate security parameters, and sound implementation of established SOM PSPs.
- Responsible for overseeing the day-to-day operability of an information system or network. This position normally carries special privileges including access to the protection state and software of a system.
- Responsible for setting up and maintaining a system or specific system elements, implements approved secure baseline configurations and conducts/assists with configuration monitoring activities as needed.

Trusted Partner

- A person (vendor, contractor, third party, etc.) or entity that has contracted or signed an agreement with the SOM to perform a service or provide a product in exchange for valuable consideration.
- IT services implemented outside information system boundaries.
- External services can be provided by entities:

    - Within the SOM but outside the authorization boundaries established for the information system; or
    - Outside the SOM either in the public or private sector.
- External information services are typically not part of SOM information systems but must meet the same applicable state and/or federal laws, rules, and regulations. Security requirements for external service providers, including the security controls for external information systems, are usually stated in contracts or other formal agreements.
- Ensures compliance requirements are met by sub-contracted service providers and third parties.

CONTROLS LISTED IN THIS POLICY

This Policy has NIST Revision 5 controls noted with an asterisk.

Heading:	Control:	Security Control Baseline:
Standard: General	AC-01; AT-01; AU-01; CA-01; CM-01; CP-01; IA-01; IR-01; MA-01; MP-01; PE-01; PL-01; PS-01; RA-01; SA-01; SC-01; SI-01; PM-01; PT-01; SR-01;	L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H; L/M/H;

TERMS AND DEFINITIONS

Access

- The ability or permission granted to individuals or entities to interact with and utilize resources, data, or functionalities of a particular system, and to enter specific physical facilities (e.g., state buildings, military establishments, and border crossing entrances).

Agency

- The principal department(s) of state government as created by Executive Organization Act, P.A. 380 of 1965.

Aggregated Data

- Data resulting from combining individual data elements into a group or category.

Attribute

- An attribute is any distinctive feature, characteristic, or property of an object that can be identified or isolated quantitatively or qualitatively by either human or automated means.

Audit Log

- A chronological record of system activities.
- Includes records of system accesses and operations performed in a given period.

Audit Trail

- A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result. The records can be used to validate the successful transfer of data or identify transfer errors as they occur.

Authorization Boundary

- All components of an Information System which share all the following characteristics are said to exist within the same Authorization Boundary:
    - Direct management control. This means having the budgetary and operational authority for the day-to-day operations and maintenance of the Information System. This corresponds to the role of the ISO in the Risk Management Framework, so it follows that, at a minimum, Information System components with different ISOs cannot be within the same Authorization Boundary.
    - Function or mission objective. This means that, at a minimum, the Information System should have at least one of the following characteristics of "who provides what to whom" a constant within the Authorization Boundary:
        - Agency (the Agency that provides the function or is responsible for the mission); or
        - Information Type (the Mission-Based Information Types in Appendix D of Volume II of [NIST SP 800-60] the Information System collects, processes, maintains, uses, shares, disseminates, or disposes); or
        - Customer (the SOM residents or workers who access the Information System to conduct the function or mission or to whom the function or mission is provided).

- Security needs. This means that, at a minimum, the entire Information System should have the same Security Controls required of it.
- General operating environment. This means that, at a minimum, the entire Information System should inherit the same Security Controls from the same General Support Systems within each of the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) layers.

Availability of Information

- Security Objective to which a Data Impact Level is assigned.
- Ensuring timely and reliable access to and use of information.
- Assuring that the systems for delivering, storing, and processing information are accessible when needed, by those who need them.

Balancing Control

- A single, or group of controls acting together, to validate that data exchanged between two systems is extracted, transformed, and loaded correctly.

Breach

- The unauthorized disclosure or acquisition of sensitive PII or other nonpublic information in physical or electronic form, if that acquisition is reasonably likely to cause substantial risk of identity theft, fraud, or compromise to the privacy and/or security of the state or resident to whom the information relates.

Break Glass

- Refers to a method of bypassing security controls that normally guard a system or service.
- The term “break glass” is a reference to someone breaking a glass stopper to pull a fire alarm. In some situations, a user may be unable to gain authorized access as they normally would.

Business Continuity Planning (BCP)

- Focuses on a particular business process.
- Must be aligned to Mission Essential Functions (MEFs).
- Does not need to be technical.
- BCP could involve manual or paper-based processes.

Business Impact Analysis (BIA)

- An analysis of an information system’s requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

  A scoring and tier scheme outlining a standard, quantitative approach to application scoring for the enterprise. Scores establish recovery priorities in

the event of a disaster and defines minimum support requirements for Michigan's Application Prioritization for Recovery list. BIA is evaluated in terms of underlying data confidentiality, service availability and data integrity requirements.

The collective evaluation produces an overall score of 1 to 10 that is used to rank the application's overall "criticality". The Service Availability score is used by DTMB to define the maximum allowable time for the application to be out of service before a serious impact to the business occurs, otherwise known as the Recovery Time Objective (RTO).

Change Builder

- A person who is responsible and accountable for the satisfactory technical completion of a specific change. Responsibilities include creating a Request for Change (RFC), managing, or executing the specific actions required to complete the change, and complying with the Agency's, including Change Management procedures.

Change Manager

- A role assigned to a specific person within an organization who is responsible for approving new RFCs, reviewing completed RFCs, and enforcing the organization's policies and processes for Change Management.

Common Control

- A security control that is inheritable by one or more organizational information systems.

Confidential Data

- Available only to authorized personnel on a need-to-know basis.
- Requires a signed non-disclosure statement.
- Applicable state and federal laws and regulations, PSPs, and privacy compliance requirements must be followed.
- May require additional security control requirements.

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Confidentiality of Information

- Security Objective to which a Data Impact Level is assigned.
- Protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.

Configuration Items

- An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process.
- Configuration items include, but are not limited to, IT services, hardware, software, buildings, people, and formal documentation such as process documentation and SLAs.

Configuration Management

- A collection of activities focused on establishing and maintaining the integrity of IT products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the System Development Life Cycle (SDLC).

Configuration Management Database (CMDB)

- A database that is used to store and manage Configuration Management Information throughout the SDLC. The database is run on a configuration management system that may contain multiple CMDB's.

Continuity of Operations Plan (COOP):

- An effort within the Executive Office to ensure that MEFs continue to perform during disruption of normal operations (FCD1, 2017, p. N-2). This is a department-level, pro-active plan that facilitates the rapid recovery of business operations to reduce the overall impact of the disaster, while ensuring the continuity of the critical business functions during and after a disaster, assuming IT is up and available. The COOP identifies MEF's of the department.

  Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The plan is needed by enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period of time. Defines the activities of individual departments and agencies and their sub-components to ensure that their essential functions are performed.

  This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the capability through tests, training, and exercises.

Continental United States (CONUS)

- The States of the United States of America, excluding Alaska and Hawaii, and including the District of Columbia.

Contractor

- A person employed either directly or under contract by any Vendor.

Criminal Justice Information (CJI)

- The subset of Information described as such in Section 4.1 of the [FBI CJIS Security Policy], or which is of one of the Information Types described in Appendices D.16 through D.18 of Volume II of [NIST SP 800-60] and designated as such by the Agency Director of the Michigan State Police.

Cryptographic Period (Cryptoperiod)

- Time span during which each key setting remains in effect.

Data

- SOM Agency information. No distinction between data and information is made in this policy.

Data Classification

- Establishes information ownership and location where data resides.
- Categorizes data's security level based on sensitivity, criticality, and risk of the information.
- Increases the confidentiality, integrity, and availability of data.

Data Impact Level

- Level assigned to data relevant to the sensitivity, criticality, and risk to the primary business function of the Agency or individuals, and potential impact of loss or compromise.

Data Mapping

- Formal documentation describing how data is properly formatted (data lineage and elements) for exchange between two interfacing systems.

Data Sharing Agreement

- An Agreement between parties that outlines how shared data will be used, disclosed, and protected, by agreeing to provisions that place general and specific limitations on the receiving party.

Data Transformation

- Conversion of a set of data values from the data format of the source system into the data format of the target system.

Data Type

- Specific category of information as defined by an Agency or specified by law, executive order, directive, policy, or regulation.
- Examples include privacy, medical, proprietary, financial, investigative, contractor sensitive, and security management.

Demilitarized Zone (DMZ)

- An IT DMZ, or perimeter network, is one or more sub-networks that are physically and logically separated from internal networks. These semi-trusted networks are designed to expose external-facing services to untrusted networks such as the Internet.

Disaster Recovery Plan (DRP)

- A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
- An IT plan that identifies all the aspects of recovering a specific application including the interdependent applications or systems, who recovers them, how they are recovered, and the durations for recovery.

Edit Controls

- Detect errors in the input portion of information that is sent to a computer for processing. The controls may be automated or manual to allow the user to edit data errors before processing.

Encryption

- The cryptographic transformation of data to produce ciphertext.
- Conversion of plaintext to ciphertext through the use of a cryptographic algorithm for the purpose of security or privacy.

External Information System (or Component)

- Information systems or components of information systems for which the SOM typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (See also Privately Owned.)

External Information System Service

- Information system service that is implemented outside of the authorization boundary of the SOM for which the SOM typically has no direct supervision or authority over the application of required security controls or assessing control effectiveness.

Federal Tax Information (FTI)

- FTI consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control that is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC § 6103(p)(4) safeguarding requirements including IRS oversight.
- FTI is categorized as Sensitive But Unclassified (SBU) information and may contain PII.
- FTI includes information received directly from the IRS or obtained through an authorized secondary source such as Social Security Administration (SSA),

Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS) or Centers for Medicare and Medicaid Services (CMS) or another entity acting on behalf of the IRS pursuant to an IRC § 6103(p)(2)(B) Agreement.

General Support System

- An interconnected set of information resources centrally managed services that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

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.

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. An instance of an information type.

Information Security

- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. For this policy, information is not limited to data in computer systems, but includes data wherever it resides in the agency, what form it takes (e.g. electronic, printed, etc.), whatever technology is used to handle it, or whatever purpose it serves.

Information Spillage

- An occurrence where either classified or nonpublic information is inadvertently placed or transferred onto information systems that are not authorized to process such information.

Information System

- A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Combination of interacting elements organized to achieve one or more stated purposes.

Information Technology (IT)

- Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data, video, voice, or information by the agency. For purposes of this definition, such services or

equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product.

IT includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, Internet of Things (IOT) devices, telecommunications equipment, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources.

The determination of whether something falls under IT is not dependent on cost (i.e., could be a free service). This definition also includes set of information technology components within an Authorization Boundary that collects, processes, maintains, uses, shares, disseminates, or disposes of State Data or Information.

Information Technology (IT) Resources

- IT assets including, but not limited to, devices, networks, data, software, hardware, email, system accounts, and facilities provided or contracted for conducting official SOM business.

Information Type

- Specific category of information as defined by an Agency or specified by applicable state and/or federal laws, rules, and regulations. Examples includes privacy, medical, proprietary, financial, investigative, contractor sensitive, and security management.

Integrity of Information

- Security Objective to which a Data Impact Level is assigned.
- Maintaining the intrinsic validity of information and assurance that the information can be relied on to be sufficiently accurate by guarding against improper information modification or destruction to ensure information has not been altered by unauthorized people.

Interconnection Security Agreement (ISA)

- An agreement established between organizations that own and operate connected IT systems to document the security responsibilities for the protection and handling of exchanged data, services offered, user community, topographical drawings, data flow and exchange method, etc.

Interface

- A connection between two devices, applications, or networks, or common boundary between independent systems or modules where interactions take place.

Internal Data

- Internal data is information that is not sensitive to disclosure within the Agency. By default, data created, updated, or stored by the Agency is considered to be internal information intended for use by Agency employees and authorized non-Agency employees, although it may be accessed by trusted partners covered by a non-disclosure agreement. This information shall be shared internally to further internal operations, lower costs, prevent duplication, and otherwise enhance the condition or operation of Agency systems.

Internet of Things (IOT)

- Objects with electronic components that include processing and networking capabilities designed to enhance the functionality of the object by leveraging communications over the internet.

Investigation Log

- A chronological document used to capture a record of events before, during, and after an incident or problem.

IT Environment

- Hardware: Routers, personal computers, servers, switches, and data centers.
- Software: Web servers and applications that make hardware connections effective and more practical.
- Networking: Firewalls, cables, and other components which facilitate internal and external communication.

ITIL v3 (Information Technology Infrastructure Library)

- A set of comprehensive practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business.

Local Access

- Logical access to an Information System by a User through a direct connection without the use of a network.

Maintenance Activity

- Any act that either prevents the failure or malfunction of Information System Components which are designated by the ISO as impacting the Availability of the Information System in the event of their failure or malfunction or restores their operating capability.

Major Incident

- An incident that results in significant disruption to the business. May include the interruption of an essential IT service or impact a large number of clients. (Examples: Virus outbreak, power outage, major security breach as defined

by CIP, evacuation of a state office building, disruption to enterprise storage services).

Major Problem

- A Problem Record identified and created to find the cause of one or more incidents. “Major” refers to the severity of that Problem. A Major Problem is used when an in-depth Root Cause Analysis or thorough Trend Analysis has been requested by an Agency and/or DTMB - Agency Services. This classification requires a Problem Resolution Team, Problem Resolution Owner (PRO) and Problem Manager be assigned.

Major Problem Review

- The review process at the end of a major problem resolution that brings together the key participants in resolving the problem.

Memorandum of Understanding (MOU)

- An agreement established between parties outlining the terms and details of an understanding, including each parties’ requirements and responsibilities. An MOU is often the first stage in the formation of a formal contract.

Mobile Device

- A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source.
- Examples include, but are not limited to: laptops, tablets, mobile phones, smartphones, personal data assistants (PDA), audio recorders and players, personal digital assistants, external hard drives, flash drives, and digital cameras. Special consideration may be made to exempt purpose-built devices that are designed to work without encryption (i.e. body cameras, medical devices, etc.).
- For the SOM, all non-state-owned computing or data storage equipment (e.g., personal computer (PC), Network Attached Storage (NAS), and Storage Area Network (SAN)) are considered mobile devices.

Monitoring Control

- Activity management performed to gain assurance that implemented controls are being performed and are operating effectively.
- Repeated observation of a control implementation to detect events and to ensure that the current status is known.

Multifactor Authentication

- Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something

you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Nonpublic Information

- Data of such nature that its loss, misuse, compromise, or unauthorized access to or modification of, can significantly harm an individual or the SOM.
- Must be protected from unauthorized access to safeguard the privacy or security of individuals and the SOM.
- Includes nonpublic Personal Identifying Information (PII).
- Confidential nonpublic information that relates to an Agency's business.
- Nonpublic information includes but is not limited to all data which contains:
    - Information protected under the Privacy Act of 1974 and vendor proprietary information are examples of nonpublic information.
    - Personal Information, as defined by the Michigan Identity Theft Protection Act, ACT 452 of 2004.
    - Protected Health Information, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
    - Student education records, as defined by the Family Educational Rights and Privacy Act (FERPA).
    - Card holder data, as defined by the Payment Card Industry (PCI) Data Security Standard (DSS).
    - Information that is deemed to be confidential in accordance with Internal Revenue Service Publication 1075 Section 8.0, Disposing Federal Tax Information (FTI).
    - Information that is deemed to be confidential by the Criminal Justice Information Service (CJIS) Section 5.8.3 Electronic Media Sanitization and Disposal; Section 5.8.4 Disposal of Physical Media.
    - Information that is protected, governed, or restricted in some manner by a federal or state statute, agreement, rule, policy, or requirement by SOM policy from unauthorized access.

Owner

- A party that possesses the exclusive right to hold, use, benefit-from, enjoy, convey, transfer, and otherwise dispose of an asset or property.

Payment Cardholder Data (PCI Data)

- The subset of information described as "Cardholder Data" or "Sensitive Authentication Data" in Version 4.0 of the [PCI DSS].

Personal Information (PI):

- PA 452 of 2004, as amended, the Identity Theft Protection Act, defines Personal information as, a person's first name or first initial and last name in combination with any of the following data elements:
    - Social Security Number
    - Driver's license number or State Personal identification card number
    - Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to a person's financial account.

Personal Identifying Information (PII):

- PA 452 of 2004, as amended, the Identity Theft Protection Act, defines Personal identifying information as, "a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, any other account password in combination with sufficient information to identify and access the account, automated or electronic signature, biometrics, stock or other security certificate or account number, credit card number, vital record, or medical records or information."

Plan of Action and Milestone (POAM)

- Created during the implementation phase of the SDLC and is updated along with the SSP and Risk Assessment until all tasks have been completed.
- Describes specific measures planned to correct weakness or deficiencies identified in the risk assessment.
- Addresses known vulnerabilities in the information system.
- Details the ISO and Authorizing Official's risk response.
    - Proposed risk mitigation approach.
    - Rationale for accepting risk.
    - Responsible party for risk mitigation.
    - Date due and date complete.
- Based on the recommended corrective action and level of risk, the ISO, IO, and Authorizing Officials may:
    - Mitigate the risk by implementing the recommended security controls.
    - Accept the risk.

- Transfer the risk, by obtaining insurance to cover potential losses.
- Transfer the risk to another organization.
- Avoid the risk by ceasing the activity that is presenting the risk or never engaging in the activity.

Privately-Owned

- Resources not purchased or leased by the SOM or being used under the provisions of a signed contract with a vendor/third-party for the SOM. (See also External Information System.)

Privileged Account

- An information system account with authorizations of a privileged user.

Privileged Command

- A direct or indirect human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

Privileged Functions

- Functions requiring authorization such as establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities.

Privileged User

- A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (Examples include [but are not limited to]: application upkeep, system administration, user or account access management, certificate or cryptographic key management, server database administration, and network infrastructure changes and security infrastructure management).

Problem

- The cause of one or more incidents. A cause is not usually known at the time a problem is identified. Restoring normal information service levels will normally take priority over investigating and diagnosing problems when possible.

Problem Manager

- The Problem Manager is the role responsible for managing individual Problem Investigations through the resolution process and ensuring that all activities within the process are followed.

Problem Resolution Owner (PRO)

- The PRO supports the Problem Manager with leadership authority and knowledge of a particular domain (technical, business or application).

Public Data

- Information explicitly approved for distribution to the public.
- Can be disclosed to anyone without violating an individual's or organization's right to privacy or causing potential harm.

Public Facing Devices

- Includes any systems that directly or indirectly receive network connections that are initiated over untrusted networks (the internet). The use of web application firewalls or other security tools does not allow for the removal of the protected devices from this compliance category.

Regulated Information Systems

- Any information system that must comply with regulatory compliance frameworks such as CJIS, IRS Pub 1075, MARS-e, PCI DSS, HIPAA, et al. If you must comply with a regulatory framework then you are being regulated.

Restart and Recover Procedure

- The actions necessary to restore a system's data files and computational capability after a system failure or penetration.

Restricted Data

- Restricted data is information that is extremely sensitive, and any disclosure or corruption could be hazardous to life or health, cause extreme damage to integrity or image, and/or impair the effective delivery of services.
- Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact.
- Restricted data can be made available to named individuals or specific positions on a need-to-know basis.
- Disclosure or corruption could be hazardous to life or health, cause extreme damage to integrity or image, or impair the effective delivery of services.
- Made available to named individuals or specific positions on a need-to-know basis.

Risk Assessment

- Provides an objective analysis of the system-specific and common controls identified in the SSP.
- Determines if controls were implemented and meeting the identified security requirements.
- Initial risk assessment is created during the construction phase of the SDLC.
- Updated annually or whenever changes are made to the security controls implemented.

    - Updates to the risk assessment ensure that the ISO, IO, and Authorizing Officials know of the security state of the information system.
- Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
- Required for the System Authorization Package.
- Does not assess security controls to determine if they are operating correctly or producing the desired outcome.

Root Cause Analysis

- A method of problem solving used for identifying and documenting the root causes of incidents or problems.

Secure Facility

- A facility designated as such in the SOM 1340.00.120.01 Physical and Environmental Protection Standard; or
- A criminal justice conveyance as defined in the FBI CJIS Security Policy Standard, when managed by the Office of Support Services and operated by a member of the Michigan State Police or a conservation officer of the Department of Natural Resources as described in [MCL 28.6], [MCL 28.6a], or [MCL 28.6d].

Security Assessment

- SOM grants access to its facilities, provides network access, outlines detailed information about the network and security plans, etc. to study security and identify improvements to secure the systems.
- Ensures that necessary security controls are integrated into the design and implementation of the project under assessment.
- Provides documentation outlining any security gaps between a project designs and approved corporate security policies.

Security Authorization Package

- Documentation that includes the SSP, Risk Assessment, and POAM.
- Used by Authorizing Officials to make risk-based decisions to permit or deny system operations.

Security Categorization

- The process of determining the security category for information or an information system.
- Basis for determining proper security controls to protect information.
- Based on Data Impact Level and Security Objective.

Security Category

- The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

Security Controls

- Management, operational, and technical controls, (e.g., safeguards or countermeasures) required for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Control Baseline

- The set of minimum-security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.

Security Objective

- Confidentiality, integrity, or availability.

Security Plan

- Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

Security-Relevant Information

- Any information within information systems that can potentially impact the operation of security functions or the provision of security services that could result in failure to enforce system security policies or maintain the isolation of code and data.
- Includes filtering rules for routers and firewalls, cryptographic key management information, configuration parameters for security services and access control lists.

Service Criticality

- Service Criticality identifies the importance of a service and is key to the incident management process. The SOM has three identified levels of criticality:
    - Critical – Business function/application outage has the potential to cause loss of life or risk of injury to a citizen. Availability is identified as 7 x 24 x 365.
    - High – Business function/application outage directly impacts the public, a large number of users are down, or the business function is politically sensitive. Availability is defined as 7 x 24 x 365.

- Medium – Business function/application that does not meet the Critical or High criteria. There is no risk of personal injury and the public is not being directly affected. Availability is identified as M-F x 8-5.

Solution Review

- The process of reviewing a Problem Solution where the solution is verified by the Business Owner and key stakeholders before the Problem Investigation is resolved.

SOM Authorities

- A Supervisor, Manager, or Agency Director, a SOM employee acting on behalf of CIP, or law enforcement.

SOM-Owned

- SOM purchased or leased resources, or vendor / third-party owned and used resources under the provisions of a signed contract with the SOM.

Source System

- IT system from which data is extracted and transferred to a target system as part of an interface transaction. Typically, the system of record for the interface is the source system.

Staff Augmentation Contractor

- Staff hired through a staff augmented vendor (i.e. Knowledge Services).
- Given direct access to SOM network (i.e. VPN, active directory, etc.).
- Given direct access to SOM proprietary information and information systems.

Standard Operating Procedure 12 (SOP 12)

- Procedures used by IT Operations to provide step by step instructions to assign, escalate, and communicate DTMB incidents and problems.

Standard Problem

- A Problem Record identified and created to find the cause of one or more incidents. “Standard” refers to the severity of that Problem. A PRO is not needed when a problem is classified as a Standard Problem.

System Security Plan (SSP)

- Overview of the information system and security requirements including:
  - Information assets
  - Security categorization
  - Applicable laws and regulations
  - System interconnections
  - Information sharing

- System dependencies
- Network diagrams
- Network devices and components
- System hardware
- System software
- Data flow diagrams
- Implementation of the security controls

- Describes the controls in place or planned to be in place required to provide the appropriate level of security.
- Required for the System Authorization Package.

Target System

- IT system that receives and loads data transferred from a source system as part of an interface transaction.

Trend Analysis

- Analysis of data to identify time-related patterns. A trend is three or more incidents within a period of time or a chronic problem that has been identified by management.

User Location

- Information that can be determined by information systems, such as internet protocol (IP) addresses from which network logons occurred, device identifiers, or notifications of local logons.

Validation Control

- Controls designed to provide reasonable assurance (1) that all records or transactions actually occurred, relate to the entity, and were properly approved by management, and (2) that output contains only valid data.

Vendor

- Any entity which has a contract through DTMB Central Procurement, (or any agency or division that has received delegated authority from DTMB Central Procurement) to provide hardware, software, services, or any other consideration other than staff augmentation to the Organization.

REFERENCES

Administrative Guide to State Government

Administrative Guide Policy 1305 Enterprise Information Technology

FBI CJIS Security Policy

MCL 28.6

MCL 28.6a

MCL 28.6d

NIST Computer Security Resource Center

NIST Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (nist.gov)

NIST Security and Privacy Controls for Information Systems and Organizations (nist.gov)

SOM IT Technical Policies, Standards and Procedures

SOM 1305.00.01 IT Policy Administration Standard

SOM 1305.00.02 Policy and Product Exception Process Standard

SOM 1305.00.02.01 Technical Review Board (TRB) and Executive Technical Review Board (ETRB) Exception Procedure

SOM 1340.00.120.01 Physical and Environmental Protection Standard

SOM 1340.00.150.02 Data Classification Standard

AUTHORIZATION

Authority

- This policy obtains its authority from:
  - Administrative Guide Policy 1305 Enterprise Information Technology.
  - The Administrative Guide to State Government.
  - SOM IT Technical Policies, Standards and Procedures.

Enforcement

- All enforcement for this policy must comply with the standards and procedures of Administrative Guide Policy 1305 Enterprise Information Technology.

Developing Standards and Procedures for this Policy

- All requirements for developing standards and procedures for this policy must comply with Administrative Guide Policy 1305 Enterprise Information Technology.

Exceptions

- All exception requests to this policy must be processed in compliance with Administrative Guide Policy 1305 Enterprise Information Technology.

Effective Date

- This policy is effective unless otherwise noted, upon signature of the Administrative Guide approval memo by the DTMB Director.