POLICY 1340.00 Information Technology Information Security

Issued: April 12, 2007
Revised: February 28, 2020
Reviewed: January 12, 2021
Next Review Date: January 12, 2022

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 policies, standards, and procedures to maintain suitable levels of enterprise-wide security.

To secure the enterprise IT environment, CIP has selected the cybersecurity framework published by the National Institute of Standards and Technology (NIST) Special Publication 800.53, Security and Privacy Controls for Federal Information Systems and Organizations (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) (Revision 4 – moderate controls) from the NIST Computer Security Resource Center (https://csrc.nist.gov/publications/sp), as the minimum security controls for all SOM IT. Each System Security Plan will address NIST security standards and guidelines including any additional controls if required in the following policies and corresponding standards.

PURPOSE

CIP is committed to securing SOM assets and provides the NIST security framework for developing, implementing and enforcing security policies, standards, and procedures 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)
Michigan Cyber Security (MCS)

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 (PSP). 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.

Policies, standards and procedures 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: Inside Michigan.gov - IT Technical Policies, Standards & Procedures (https://stateofmichigan.sharepoint.com/teams/insidemi/Pages/For%20Your%20Job/In%20the%20Office/IT_PSP.aspx).

SOM or environmental changes may require changes to this security policy. Any efforts to request, approve, implement, or communicate changes to policies, standards, or procedures that this policy regulates or governs must be made under SOM 1305.00.01 IT Policy Administration Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1305.00.01%20IT%20Policy%20Administration%20Standard.pdf).

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 SOM 1305.00.02 Technical Policy and Product Exception Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1305.00.02%20Technical%20Policy%20and%20Product%20Exception%20Standard.pdf) and SOM 1305.00.02.01 Technical Review Board (TRB) and Executive Technical Review Board (ETRB) Exception Procedure (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1305.00.02.01%20Technical%20Review%20Board%20and%20Executive%20Technical%20Review%20Board%20Exception%20Procedure.pdf).

CIP will duly implement and enforce security policies, standards, and procedures 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.

STANDARDS

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 policy, security standard, and procedure must be reviewed and optionally, updated annually.

020 Access Control (AC-1)

SOM 1340.00.020.01 Access Control Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.020.01.01%20Remote%20Vendor%20Access%20Procedure.pdf) establishes the Access Control standards in this SOM policy.

These standards require security controls, authorized access and use of information systems, special and limited access conditions, physical and automated process monitoring, and authorized system account activities by approved personnel. These standards ensure that SOM Authorizing Officials and all other associated personnel understand the responsibilities, access management requirements, and separation of duties necessary to effectively manage information system accounts; and coordinate, plan, and execute appropriate physical and account access control activities.

030 Security Awareness and Training (AT-1)

SOM 1340.00.030.01 Security Awareness and Training Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.030.01%20Security%20Awareness%20and%20Training%20Standard.pdf) establishes the Security Awareness and Training standards in this SOM policy.

These standards require role-specific training on security controls, authorized access and use of information systems, physical and process monitoring, and authorized system activities and functions by approved personnel. These standards ensure that SOM Authorizing Officials and all other associated personnel understand the responsibilities and training requirements necessary to effectively maintain organizational awareness, minimize insider threats, and prevent additional security related incidents.

040 Audit and Accountability (AU-1)

SOM 1340.00.040.01 Audit and Accountability Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.040.01%20Audit%20and%20Accountability%20Standard.pdf) establishes the Audit and Accountability standards in SOM policy.

These standards require approved personnel to audit essential information, manage audit service devices and locations, integrate audit events, manage audit repositories, and process and generate audit reports. These standards ensure that SOM Authorizing Officials with auditing responsibilities understand the responsibilities required to successfully manage audit information, assign audit roles and tasks, and prevent the compromise of SOM information.

050 Security Assessment and Authorization (CA-1)

SOM 1340.00.050.01 Security Assessment and Authorization Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.050.01%20Security%20Assessment%20and%20Authorization%20Standard.pdf) establishes the Security Assessment and Authorization standards in SOM policy.

These standards require approved personnel to conduct impartial security and organizational assessments, establish external system restrictions, and conduct penetration testing and other necessary vulnerability assessments. These standards ensure that SOM Authorizing Officials and all other associated personnel understand the responsibilities necessary to establish effective security assessment and authorization controls, prevent conflicts of interest, and maintain continuous monitoring strategies.

060 Configuration Management (CM-1)

SOM 1340.00.060.01 Configuration Management Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.060.01%20Configuration%20Management%20Standard.pdf) establishes the Configuration Management standards in SOM policy.

These standards require approved personnel to adequately manage the configuration of SOM's configuration systems, including retaining previous system configurations, configuring approved devices for high-risk areas, tracking and documenting system changes, and assigning privileges to authorized personnel. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to maintain up-to-date system configuration, support rollbacks and system change requirements, and prevent unauthorized system changes, including software or program installations.

070 Contingency Planning (CP-1)

SOM 1340.00.070.01 Contingency Planning Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.070.01%20Contingency%20Planning%20Standard.pdf) establishes the Contingency Planning standards in SOM policy.

These standards require approved personnel to coordinate contingency plans with existing organizational contingency development, designate key resumption

activities, define service-level priorities, and define critical assets and offsite backup sites, including telecommunications, transaction systems and operational separation measures. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to prevent conflicts with other organizational contingency elements, effectively resume essential operations during and after a disruption, prevent loss or compromise of assets, and provide alternate methods to secure, store and access SOM information.

080 Identification and Authentication (IA-1)

SOM 1340.00.080.01 Identification and Authentication Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.080.01%20Identification%20and%20Authentication%20Standard.pdf) establishes the Identification and Authentication standards in SOM policy.

These standards require personnel to manage network systems that employ multifactor and public key information (PKI)-based authentication, replay-resistant mechanisms, identification of connected devices, and registration process requirements. These standards ensure that SOM Authorizing Officials and third parties understand the responsibilities necessary in order to regulate non-privileged access of SOM accounts, minimize authentication attacks, and prevent unauthorized devices and connections with SOM networks.

090 Incident Response (IR-1)

SOM 1340.00.090.01 Incident Response Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.090.01%20Incident%20Response%20Standard.pdf) establishes the Incident Response standards in SOM policy.

These standards require approved personnel to apply incident response capabilities, including response and reporting processes, establish a test process for those incident response capabilities, and coordinate with existing SOM contingency plans. These standards ensure that SOM Authorizing Officials and all other associated personnel understand the responsibilities necessary to ensure the SOM's incident response capability is effective, prevents conflicts with other organizational contingency elements, and relies on system response, reporting, and support.

100 Maintenance Policy (MA-1)

SOM 1340.00.100.01 Maintenance Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.100.01%20Maintenance%20Standard.pdf) establishes the Maintenance standards in SOM policy.

These standards require approved personnel to employ adequate and approved information maintenance tools, inspect all maintenance tools entering SOM facilities, including supporting media, and apply priority or time-sensitive maintenance procedures. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to effectively diagnose and repair SOM information systems, ensure maintenance tools and supporting media are not modified beyond the SOM's authorized specifications, and determine the levels

of risk and priority for each particular information system affected during an incident.

110 Media Protection (MP-1)

SOM 1340.00.110.01 Media Protection Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.110.01%20Media%20Protection%20Standard.pdf) establishes the Media Protection standards in SOM policy.

These standards require all SOM personnel to apply proper information system media markings on all approved media, devices, and systems property; properly designate and control both physical and digital storage locations; execute approved and secure transport methods; ensure cryptographic protection is applied to required devices; and prohibit the use of unidentifiable devices. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to ensure all SOM media is adequately used, handled, and distributed and also properly protected, stored, and transported, including applying additional security mechanisms and restrictions on the use of unauthorized media devices.

120 Physical and Environmental Protection (PE-1)

SOM 1340.00.120.01 Physical and Environmental Protection Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.120.01%20Physical%20and%20Environmental%20Protection%20Standard.pdf) establishes the Physical and Environmental Protection standards in SOM policy.

These standards define both physical facility and information system management processes. All corresponding personnel will apply and manage security safeguards accordingly for facilities and information system distribution and transmission lines; control and monitor physical information output devices and locations, including the use of safety, intrusion and surveillance equipment; and implement appropriate power protection and alternate location practices and measures. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to prevent unauthorized communication or transmission access, maintain access records, minimize the compromise of sensitive output information, and protect SOM equipment, facilities and environments, including emergency power procedures and relocation contingencies.

130 Security Planning (PL-1)

SOM 1340.00.130.01 Security Planning Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.130.01%20Security%20Planning%20Standard.pdf) establishes the Security Planning standards in SOM policy.

These standards require assigned SOM personnel to effectively coordinate security related activities with other organizations and outside entities, provide and enforce social media and network rules and restrictions, and implement a compliant information security architecture. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to prevent security

activity conflicts within and throughout the SOM, prevent negative impact and restraints on other organizations, minimize unauthorized access to SOM information available on public information sites, and ensure a compliant security architecture is in place and is continuously assessed.

140 Personnel Security (PS-1)

SOM 1340.00.140.01 Personnel Security Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.140.01%20Personnel%20Security%20Standard.pdf) establishes the Personnel Security standards in the SOM policy.

These standards require that the organization employs mechanisms to control both SOM personnel and third-party providers of employee transfers, commencement and termination status, including disabling access for specific information systems, designating a risk status for specific positions and roles, and conducting personnel screening before granting authorization or access. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to ensure that appropriate personnel have limited or appropriate access, that changes in personnel status properly control further access or restriction to information systems, and that appropriate documentation and processes are followed to track corresponding authorization changes and access.

150 Risk Assessment (RA-1)

SOM 1340.00.150.01 Risk Assessment Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.150.01%20Risk%20Assessment%20Standard.pdf) establishes the Risk Assessment standards in SOM policy.

These standards require that appropriate vulnerability scanning tools are employed, accurate updates of scanned vulnerabilities are maintained, and legitimate vulnerabilities are remediated. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to readily identify and respond to system vulnerabilities.

160 System and Services Acquisition (SA-1)

SOM 1340.00.160.01 System and Services Acquisition Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.160.01%20System%20and%20Services%20Acquisition%20Standard.pdf) establishes the System and Services Acquisition standards in SOM policy.

These standards require that the organization applies visually functional security interface controls; controlled levels of systems design and implementation; and appropriate systems engineering, configuration, and service principles. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to ensure that SOM sensitive information is excluded from open and unauthorized view, that system functionality and requirements are defined during early development, and that proper process life-cycle strategies are in place.

170 System and Communications Protection (SC-1)

SOM 1340.00.170.01 System and Communications Protection Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.170.01%20System%20and%20Communications%20Protection%20Standard.pdf) establishes the System and Communications Protection standards in SOM policy.

These standards require that the organization employs application, information, and functionality partitioning measures, limits external network connection points, properly manages external telecommunications, prevents unauthorized connections, and secures and monitors all transmitted and stored data, including all channeling networks. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to prevent unauthorized system management access and control information flow via shared information sources, connections, networks, and other data sources.

180 System and Information Integrity (SI-1)

SOM 1340.00.180.01 System and Information Integrity Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.180.01%20System%20and%20Information%20Integrity%20Standard.pdf) establishes the System and Information Integrity standards in SOM policy.

These standards require that the organization employs mechanisms that alert the organization and identify information system flaws during malfunction or failure, designates management procedures for malicious code protection measures, applies near real-time event analysis, validation, and verification tools, including traffic communications monitoring, and logs detected events for use in contingency planning. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to effectively determine changing states within the SOM's information systems, obtain accurate event-based system information, and determine suitable corrective actions for security-relevant events.

ROLES AND RESPONSIBILITIES

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 (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.150.02%20Data%20Classification%20Standard.pdf).
    - Data management complies with federal and state laws and 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 identification and classification of data. Although it is not recommended to have multiple owners for the same data, this sometimes occurs. Where there is more than one owner, Information Owners must designate a Business Owner who has authority to decide for all owners of the 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 System Security Plans.
- Ensures internal Agency security policies and procedures are implemented, maintained and enforced that compliment and comply with this policy.
- Ensures Agency employees and Trusted Partners handle information for which they are responsible in compliance with this policy and all applicable SOM policies.
- Ensures all Agency employees are trained to handle information in accordance with this and all SOM policies.
- 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 policies than those developed by DTMB for the SOM in conjunction with DTMB.

Agency Authorizing Official (Delegated Authority)

- Authorizes operation of and budgetary oversight for an information system.
- Assumes responsibility for the mission and business operations supported by the system.
- Assumes responsibility for operating an information system at an acceptable level of risk to the Agency's operations, assets or individuals.

- Assumes accountability for the security risks associated with the information system operations.
- Approves System Security Plans, memoranda of agreement, and each Plan of Action and Milestones (POAMs).
- Denies authorization to operate the information system if unacceptable security risks exist.
- Issues an interim authorization to operate the information system under specific terms and conditions.
- Coordinates activities with Agency Security Officers, Common Control Providers, Information System Owners, Information Owners, Information Security Officers, and DTMB officials.
- If an information system has multiple Agency Authorizing Officials, establishes agreements among them and documents them in the information System Security Plan.

Agency Authorizing Official Designated Representative

- Acts for an Agency Authorizing Official to coordinate and conduct the required day-to-day activities associated with the security authorization process.
- As authorized by Agency Authorizing Officials, makes decisions on planning and resourcing of the security authorization process, approval of the System Security Plan, approval and monitoring the implementation of POAMs, and assessment and determination of risk.
- Cannot authorize an information system to operate or approve POAMs.

Agency Security Officer

- Assists the Agency Information System Owners, Information Owners and Agency Authorizing Official in ensuring that information systems have adequate security controls in place to meet all state and federal laws, regulations and policies.
- May administer an Agency information security program or serve as the Agency Authorizing Official Designated Representative or Security Control Assessor.
- May serve as primary liaison between the Agency and DTMB, Data Custodians, Common Control Providers and External Service Providers.
- Ensures and maintains the appropriate operational security posture of Agency information systems.
- May assist in the development and compliance of security policies and classifying information assets.
- May assist the Information System Owner and Information Owner in completing the System Security Plan and POAM.
- Reviews and responds to security notifications from the Michigan Security Operations Center.

- Serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system.
- Oversees an information system's physical and environmental protection, personnel security, incident handling, and security training and awareness.
- Oversees the implementation of security awareness training within the Agency.
- Works with the Statewide Security Awareness Coordinator to implement statewide general security awareness programs in the Agency.
- Ensures that appropriate role-based training materials are timely developed for intended Agency audiences.
- Assists Agency managers in establishing a tracking and reporting strategy for security training.

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 Information System Owner and Information Owner in completing the System Security Plan and POAM.

DTMB

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 Chief Security Officer (CSO) to develop and maintain a statewide Cybersecurity and Infrastructure Protection program to fulfill the Director's responsibilities for system security planning.
- Ensures that Agency Directors, Agency Authorized Officials, Information System Owners, Information Owners, Data Custodians, and other related personnel understand the concepts and strategy of the IT/cybersecurity program.

- Ensures that Agencies have access to SOM policies, standards, procedures 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 policies.
- 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 Information Technology, IT Network and Infrastructure, and Configuration Management.
- Directs the activities necessary to keep the technology infrastructure efficient and effective while ensuring compliance with established policies, standards and procedures.
- 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 System Security Plans with Information System Owners, DTMB Information System Security Officers, and Agency Authorizing Officials.
- Ensures that personnel with significant responsibilities for System Security Plans are trained.
- Assists senior Agency officials with their responsibilities for System Security Plans.
- Ensures the policies defined in the Cyber Security Program align with the enterprise information security program.
- Develops and maintains data classification policies, procedures 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, policies, standards, and other authoritative documents.
- Oversees the creation, maintenance, and enforcement of established enterprise information security policies, standards, procedures, 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, 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 policies, standards, and procedures 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.

DTMB Business Relationship Manager (BRM)

- Coordinates and conducts the required day-to-day technological management activities associated with the security authorization process.
- As authorized by the Agency Authorizing Official, may decide on the technological planning and resourcing of the System Security Plan and POAM.
- Ensures that the appropriate operational security posture is maintained for an information system working closely with the Agency Security Officers, Information System Owner, and Information Owner.
- Has the detailed knowledge and expertise required to manage the security aspects of an information system.

DTMB MCS Security Liaison

- Coordinates and facilitates completion of the System Security Plan, Risk Assessment and POAM for an Agency.
- Works closely with the DTMB Information System Security Architects, Information System Owners, Information Owners, Agency Security Officers, Common Control Providers and Data Custodians on security-related issues and services.

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 System Security Plan.
- 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.
    - Provide support for understanding security alerts and notifications.

- Potential adverse effects of identified vulnerabilities.
- Support MCS objectives on enterprise teams and committees.

Statewide Security Awareness Coordinator

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

Information System

Information System Owner

- The Information System Owner has the following responsibilities for System Security Plans:
  - Develops the System Security Plan in coordination with the Information Owner, system administrator, DTMB Information System Security Officer, Common Control Provider, Security Liaison, 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 (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.150.02%20Data%20Classification%20Standard.pdf), and other standards encompassed by this policy.
  - Maintains the System Security Plan 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 System Security Plan when a significant change occurs.
  - Assists in identifying, implementing, and assessing the common security controls.
- Based on guidance from the Agency Authorizing Official creates and maintains the POAM.
- Based on guidance from the Agency Authorizing Official, 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.
- Coordinates with CIP on assembling and submitting the authorization package to the Authorizing Officials identified in the System Security Plan.
- Permits and documents information from multiple Information Owners, if applicable.

Information Owner

- Establishes the rules for appropriate use and protection of the subject data or information.
- In coordination with the Information System Owner, categorize the information system based on FIPS 199, NIST SP 800-60, SOM 1340.00.150.02 Data Classification Standard (https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.150.02%20Data%20Classification%20Standard.pdf) and other standards encompassed by this policy.
- Provides input to Information System Owners 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.

Data Custodian

- Implements and manages the necessary safeguards to protect data based on requirements established by the Information System Owner and documented in the System Security Plan.
    - Protects the information from unauthorized access.
    - Performs backup and recovery functions.

Common Control Provider

- Documents organization-identified common controls in a System Security Plan, ensuring that a security risk assessment is performed by appropriate personnel and a POAM is produced.
- Informs Information System Owners when problems arise in inherited common controls.
- Maintains compliance for common controls with applicable federal, state, and agency security controls of all systems inheriting the common controls.

Roles

Agency

- Gathers data, enters it into the system, verifies its accuracy, specifies why it can or will be used, designates who can use it, and ultimately fills a business need for its use.

Business Owner

- Designated by Information Owners when multiple Information Owners own the same information.
- Makes decisions for all owners of this data.
- Administers systems and may be delegate to the System Administrators.
- Usually owns the primary business functions served by the application and is the application's largest stakeholder.

Managers and Supervisors

- Comply with IT security awareness and training requirements established for their users.
- Work with their Agency Security Awareness Coordinator to meet shared responsibilities.
- Serve in the role of System Owner and Data Owner, where applicable.
- As authorized by the Information Owner, may handle the day-to-day security operations of a system.
- Consider developing individual development plans (IDPs) for employees with significant 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.

Trusted Partner

- Information technology services implemented outside information system boundaries.
- External services can be provided by entities (1) within the SOM but outside the authorization boundaries established for the information system or (2) 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 federal and state laws, regulations, executive orders, directives, policies, and standards. 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.

Users

- Includes all state employees, contractors, guests, visitors, other collaborator 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.
- Trained in the rules of behavior for the systems and applications to which they have access.
- Works with management to meet training needs.
- Keeps software and applications updated with security patches.
- 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.

System Security Glossary

Agency

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

Aggregate Data

- Data resulting from combining individual data elements into a group or category.
- May become sensitive data as a result of combination.

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.

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 personally identifiable or other sensitive 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.

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 an RFC, managing or executing the specific actions required to complete the change, and complying with the organization's policies and procedures, 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.

Common Control Provider

- An organization official responsible for developing, implementing, assessing, and monitoring common controls inherited by an information system (i.e., security controls inheritable by 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, policies, standards, procedures 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 Service Level Agreements (SLA).

Configuration Management

- A collection of activities focused on establishing and maintaining the integrity of information technology 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.

Configuration Management Database (CMDB)

- A database that is used to store and manage Configuration Management Information throughout the system development life cycle. 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 mission essential functions (MEF) 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.

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 Custodian

- An individual, team, or organization delegated by an Information System Owner that has operational responsibility for technological management of information systems and 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 information technology 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

- 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.

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

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

Information Owner

- Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. This official is ultimately responsibility for ensuring the protection and use of data.

Information Security

- 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 (electronic, printed, etc.), whatever technology is used to handle it, or whatever purpose it serves.

Information Spillage

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

Information System Owner

- Official responsible for the overall procurement, development, integration, modification, operation, maintenance, and disposal of an information system.

Information Technology

- 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. Information technology 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).

Information Technology (IT) Resources

- Information technology 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 law, executive order, directive, policy, or regulation. 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. The ISA also supports the use of a Memorandum of Understanding between the organization.

Interface

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

Internal Data

- Information created, updated, or stored by the Agency that is not sensitive to disclosure within the Agency.

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.

ITIL v3 (formally an acronym for 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.

Major Incident

- An incident that 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 a BRM, I&OM or staff in a higher position. This classification requires a Problem Resolution Team, Problem Resolution Owner 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

- Any portable computing and communications device (state-owned or privately-owned) capable of accessing data, storing data, or processing data or information. Examples include, but are not limited to: laptops, tablets, mobile phones, smartphones, personal data assistants (PDA), audio recorders and players, personal digital assistants, and digital cameras. Special consideration may be made to exempt purpose-built devices that are designed to work without encryption (body cameras, medical devices, etc.).

- For the SOM, it includes all non-state-owned computing or data storage equipment (e.g., personal computer (PC), server, Network Attached Storage (NAS), and Storage Area Network (SAN)) are considered mobile devices.

Portable Media

- Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory).

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

- Any information that the general public cannot access in accordance with state or federal laws, executive orders, directives, policies, regulations, standards, or guidance.
- Information protected under the Privacy Act of 1974 and vendor proprietary information are examples of nonpublic information.

Owner

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

Plan of Action and Milestone (POAM)

- Created during the implementation phase of the System Development Life Cycle (SDLC) and is updated along with the System Security Plan 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 Information System Owner 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 Information System Owner, Information Owner 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.

Portable 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. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.

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

- The Problem Resolution Owner (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.

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

- Extremely Sensitive Information.
- 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 System Security Plan.
- 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 Information System Owner, Information Owner 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.

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 System Security Plan, 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.

Sensitive 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 non-public Personal Identifying Information (PII).
- Confidential non-public information that relates to an Agency's business.
- Sensitive Information includes but is not limited to all data which contains:
    - 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.

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 Director of the owner of a portable device, 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

- Information Technology 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.

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 Problem Resolution Owner is not needed when a problem is classified as a Standard Problem.

Target System

- Information Technology 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.

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.

System Security Plan

- 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.

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.

AUTHORIZATION

Authority

- This policy obtains its authority from:
  - Administrative Guide Policy 1305 Enterprise Information Technology (https://www.michigan.gov/documents/dmb/1305_193158_7.pdf).
  - The Administrative Guide to State Government (https://www.michigan.gov/dtmb/0,5552,7-358-82547_9347---,00.html).
  - SOM IT Technical Policies, Standards and Procedures (https://stateofmichigan.sharepoint.com/teams/insidemi/Pages/For%20Your%20Job/In%20the%20Office/IT_PSP.aspx), which can be found on the Inside.Michigan Intranet.

Enforcement

- All enforcement for this policy must comply with the standards and procedures of Administrative Guide Policy 1305 Enterprise Information Technology (https://www.michigan.gov/documents/dmb/1305_193158_7.pdf).

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 (https://www.michigan.gov/documents/dmb/1305_193158_7.pdf).

Exceptions

- All exception requests to this policy must be processed in compliance with Administrative Guide Policy 1305 Enterprise Information Technology (https://www.michigan.gov/documents/dmb/1305_193158_7.pdf).

Effective Date

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

***