POLICY 1340.00 Information Technology Information Security

Issued: April 12, 2007
Revised: July 18, 2016
Next Review Date: July 18, 2017

APPLICATION

This policy is for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, Boards or Commissions using state of Michigan (SOM) information networks and information technology (IT) Resources.

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, Michigan Cyber Security (MCS) has selected the cybersecurity framework published by the National Institute of Standards and Technology (NIST) Special Publication 800.53, Assessing Security and Privacy Controls for Federal Information Systems and Organizations (http://csrc.nist.gov/publications/PubsSPs.html), (Revision 4 – moderate controls) as the minimum security controls for SOM information systems. Each System Security Plan will address NIST security standards and guidelines in the following policies and corresponding standards.

PURPOSE

MCS 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 system. This policy establishes the SOM strategic view of IT security 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 addressed in this policy and corresponding standards and procedures.
SUMMARY

Security controls 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. 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, personnel, operational, and technical issues over:

- NIST Control Families
- Data Classification
- Ownership and Transfer of SOM Information
- Authorization Prerequisites
- Acceptable Use of Information Technology
- Electronic Processing
- IT Network Infrastructure
- Database Security
- Sensitive Information

SOM or environmental changes may require changes to this security policy. Any effort 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.

Policy exceptions occur for many of 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. Any exception must be made under SOM 1305.00.02 Technical Policy and Product Exception Standard.
CIP will duly implement and enforce security policies, standards, and procedures to ensure their effective dissemination and availability. MCS may enforce compliance through audits, vulnerability scanning, and corrective actions. If an Agency does not comply with mandates in this policy and corresponding sub-level documents, the Agency, Business Owner, and Information System Owner accept the associated risks due to non-compliance.

**POLICIES**

**General**

The following SOM policies are established in accordance with corresponding NIST controls. Each SOM Agency is bound to each policy. The policies establish the standards and procedures to effectively implement corresponding SOM Cyber Security baseline controls on the subject. All SOM Agencies must develop, adopt, and adhere to a formal, documented procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among SOM entities, and demonstrates compliance with each of the following policy areas. Each policy, security standard, and procedure must be reviewed and updated annually.

**020 Access Control (AC-1)**

SOM IT Standard 1340.00.020.01 establishes the Access Control standards in this SOM policy.

These standards require automated 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 IT standard 1340.00.030.01 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 automated 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 IT standard 1340.00.040.01 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 IT standard 1340.00.050.01 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 IT standard 1340.00.060.01 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 and program installs.

070 Contingency Planning (CP-1)

SOM IT standard 1340.00.070.01 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 IT standard 1340.00.080.01 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 IT standard 1340.00.090.01 establishes the Incident Response standards in SOM policy.

These standards require approved personnel to apply incident response capabilities, including automated 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 automated system response, reporting, and support.

**100 Maintenance Policy (MA-1)**

SOM IT standard 1340.00.100.01 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 IT standard 1340.00.110.01 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 IT standard 1340.00.120.01 establishes the Physical and Environmental Protection standards in SOM policy.

These standards require definition of 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 IT standard 1340.00.130.01 establishes the Security Planning standards in SOM policy.

These standards require all 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 an adequate 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 proper security architecture is in place and is continuously assessed.

140 Personnel Security (PS-1)

SOM IT standard 1340.00.140.01 establishes the Personnel Security standards in the SOM policy.

These standards require that the organization employs automated 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 IT standard 1340.00.150.01 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 IT standard 1340.00.160.01 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 IT standard 1340.00.170.01 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 non-remote 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 IT standard 1340.00.180.01 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 central management for automated malicious code protection measures, applies 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.
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 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 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 policies.

- 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 all SOM employees and Trusted Partners handle information for which they are responsible in compliance with this policy and all SOM policies.

- Ensures all Agency employees are trained to handle information in accordance with this and all SOM policies.

- Appoints an Agency Security Training Coordinator.

- 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 stat 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

• 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 Plans of Action and Milestones (POAMs).

• Denies authorization to operate the information system or if unacceptable security risks exist.

• Issues an interim authorization to operate the information system under specific terms and conditions.

• Assigns an Agency Senior Information Security Officer and necessary Agency Security officers and Agency Privacy Officers.


• 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 Senior Information 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.

**Agency Security Officer**

• Ensures and maintains the appropriate operational security posture of the information system.

• 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.

**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.

**Agency POAM Coordinator**

• Handles continuous monitoring and updating of the POAM.

  Cannot authorize an Information System to operate or approve a POAM.

**Agency Security Training Coordinator**

• Implements 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.
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 policies, standards, procedures, 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.

**DTMB Authorizing Official**

• 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.

• Cannot approve the System Security Plan or POAM.

**MCS Authorizing Official**

• Reviews Security Authorization Packages and authorizes implementation of the information system.
• May authorize the information system to operate or deny the authorization to operate based on the level of risk to SOM operations, assets or individuals.

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.

DTMB Information System Security Officer

• 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.

• Serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system.

• Has the detailed knowledge and expertise required to manage the security aspects of an information system.

• As authorized by the Information Owner, may handle the day-to-day security operations of a system.

• Oversees an information system’s physical and environmental protection, personnel security, incident handling, and security training and awareness.

• Assists in the developing of the security policies and procedures and ensures compliance with those policies and procedures.

• As authorized by the Information System Owner and Information Owner, may play an active role in:
  o The system’s operational environment.
  o Developing and maintaining the System Security Plan.
  o Managing and controlling changes to the system.
  o Assessing the security impact of changes to the system.

DTMB Information System 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.
- Creating POAMs.
- Risk mitigation approaches.
- Security alerts.
- Potential adverse effects of identified vulnerabilities.

**Statewide Security Awareness Coordinator**
- Oversees the Statewide General Security Awareness Program.
- Ensures that appropriate general security awareness materials are timely developed for the intended audiences.
- Ensures that awareness and training material is effectively deployed to reach the intended audience.
- Ensures that Agency Awareness Coordinators have an effective way to provide feedback on the awareness and training material.
- Ensures that awareness and training material is reviewed periodically and updated as necessary.
- Assists management in establishing a tracking and reporting strategy.
- Assists Agency Security Awareness Coordinators with the enterprise program.

**Information System**

**Information System Owner**
- Agency official responsible for the overall procurement, development, integration, modification, operation, maintenance, and disposal of the information system. 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, 1340.00.150.02 Data Classification Standard, and other standards encompassed by SOM IT Policy 1340.00.
  - Maintains the System Security Plan and ensures that the system is deployed and operated according to agreed-upon security requirements.
o Decides who has access to the system and the types of privileges and access rights.

o Ensures that system users and support personnel receive required security training.

o Updates the System Security Plan when a significant change occurs.

o 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 MCS 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

• An individual or organization with (1) statutory or operational authority for specified information, (2) responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal, and (3) ultimately responsibility for ensuring the protection and use of data.

• 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 and other standards encompassed by SOM IT Policy 1340.00.

• 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

- An individual or organization delegated by an Information Owner with responsibility for technological maintenance and management of information systems and corresponding data.
- Implements and manages the necessary safeguards to protect data based on requirements established by the Information Owner and documented in the System Security Plan.
  - Protects the information from unauthorized access.
  - Performs backup and recovery functions.

Common Control Provider

- An individual, group or organization responsible for developing, implementing, assessing, and monitoring common controls inherited by an information system.
- 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.

Risk Assessment Team

- A group of individuals defined in the initiation phase of the information system to identify and document the information system security risks that is led by the MCS Security Liaison and may include DTMB Information System Security Architects, Information System Owners, Information Owners, Agency Security Officers and Subject Matter Experts.

POAM Team

- A group of individuals which may include Information Owners, Information System End Users, Common Control Providers, and support personnel such as database administrators, web administrators, programmers, DTMB Information System Security Architects or other security professionals that remediates risks documented in the POAM.

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
• 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.
• 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.

Non-privileged Users
• Individuals without appropriate authorizations.

Security Control Assessor
• An individual, group, or organization officially assigned by the Agency.
• Conducts a comprehensive assessment of the management, operational, and technical security controls employed by an information system to determine the overall effectiveness.
• Determines if controls are implemented correctly, operating as intended and producing the desired outcome.
• Prepares the final security assessment report documenting any weaknesses or deficiencies discovered.
• Recommends a corrective action plan to address identified vulnerabilities.
• Conducts an assessment of the System Security Plan to ensure security controls meet the stated security requirements.
Subject Matter Experts

- Individuals with in-depth knowledge of the system and its functions and operations, which may include information system end users and information support personnel such as database administrators, web administrators, programmers, security architects or other security professionals.

System Administrator

- Assigned by the Business Owner for the upkeep, configuration, and reliable operation of computer systems.

Trusted Partner

- A person (vendor, contractor, Third party, etc.) or entity that has contracted with the SOM to perform a service or provide a product in exchange for valuable consideration.
- 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.

Users

- Includes 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

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

**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.

**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 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.

**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 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.

External Information Systems/Non-organizationally Owned Devices

- Information systems or components of information systems outside of the authorization boundary established by the SOM.
- Information systems or components of information systems for which the SOM typically has no direct supervision or authority over the application of required security controls or assessing control effectiveness.

Information

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

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 Technology (IT) Resources

- Includes devices, networks, data, software, hardware, email, system accounts, and facilities provided to conduct 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.
Internal Data

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

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.

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.

Privileged Functions

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

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.
- Required for the System Authorization Package.
- Does not assess security controls to determine if they are operating correctly or producing the desired outcome.

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**
• Basis for determining proper security controls to protect information.
• Determined for both data type and system level.
• Based on Data Impact Level and Security Objective.

**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-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 compromise, change, misuse, or loss 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.
• Personal Identifying Information (PII)
• Confidential non-public information that relates to an Agency’s business.

**System Security Plan**
• Overview of the information system and security requirements including:
  o information assets
  o security categorization
  o applicable laws and regulations
  o system interconnections
  o information sharing
  o system dependencies
  o network diagrams
  o 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.

---

**Authorization**

**Authority**

- This policy obtains its authority from:
  - Administrative Guide Policy 1305 Enterprise Information Technology.
  - DTMB IT Technical Policies, Standards and Procedures, which can be found on the DTMB Intranet.

**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 upon signature of the Administrative Guide approval memo by the DTMB Director.