



Assumptions

It is assumed that:

1. The State will establish a MICAM project steering committee to oversee the progress of the project. This steering committee will have representation from Contractor. Additionally, Contractor may conduct periodic quality reviews on the services being delivered and the State will cooperate and participate in such reviews.
1. Deloitte & Touche LLP will perform the services in accordance with the Statement on Standards for Consulting Services issued by the American Institute of Certified Public Accountants (AICPA), which will create no obligation on the State. We will provide our observations, advice, and recommendations. However, our services will not constitute an engagement to provide audit, compilation, review, or attestation services as described in the pronouncements on professional standards issued by the AICPA, and, therefore, we will not express an opinion or any other form of assurance with respect to the State's system of internal control over financial reporting or its compliance with laws, regulations, or other matters.
2. The State will provide access to relevant documents and pre-existing project requirements gathered developed by the State, templates and related material, other resources necessary for performing the services. The State will also provide all relevant hardware, software, licenses etc. and appropriate related setup/maintenance/support for developing project deliverables.
3. The State is responsible for organizational communication of project goals and expectation management. In addition, the State is responsible for providing appropriate points of contact (for problem escalation, reporting etc.) in a timely manner.
4. Physical server maintenance for the State's hosted MICAM will be provided by the State personnel. The State will perform all internal functions such as maintenance, patches identification, patch publication and upgrades to the operating systems and problem management of the physical hardware infrastructure (for example but not limited to, servers, operating system, storage area network, routers, networks, disks).
5. The State is responsible for all customizations and configuration changes required on the target systems, authoritative sources and applications managed by MICAM to facilitate the integration with the MICAM solution i.e. ISIM and ISAM for user provisioning, access management, web single sign-on, and Federation single sign-on.
6. It is assumed for auditing and reporting requirements, out of the box (OOTB) reports provided by ISIM and ISAM will be deployed. The project scope does not entail developing and deploying any custom reports for ISIM and ISAM, or any other MICAM components.
7. Depending on the application architecture, the integration of a given application in scope of this project with ISAM for SSO may need modifications to its login mechanism. It is assumed that the State would be willing to customize/update the login mechanism as required to achieve the necessary integration. The State will provide appropriate application development/architecture staff for this purpose.
8. ISAM integration with applications for SSO will be limited to coarse grained authorization only. Target applications will be responsible for fine grained authorization. Coarse grained authorization focuses on controlling access to URL/ Page level access. Fine grained authorization focuses on securing the underlying services and data. Fine grained authorization is out of scope for this project.
9. It is assumed that out-of-the-box functionality provided by the MICAM solution components are sufficient to meet the requirements for accessibility, auditing, reporting, self-service, and provisioning.
10. Delays or unavailability of the State resources, access to various support teams, hardware or software may impact project timing and cost.
11. The integration of MICAM (ISIM, ISAM, TDI, IBM DataPower and TFIM) with target backend applications may involve deployment of software components on the target applications. Additionally, configuration



and/or customization of target applications that may be required to facilitate the integration will be performed by the State.

12. Contractor will coordinate with the solution software provider to address defects caused by the product software or third party products, and such defects shall be outside of the post-implementation support but may be addressed via the change request process using the agreed upon rate card.
13. The State will provide access to performance testing tools and sufficient licenses required to conduct performance (volume and stress) testing. Any application specific scripts that need to be developed for performing testing with the MICAM solution will be done by the State staff.
14. The State staff will be responsible for executing the User Acceptance Testing (UAT) for the MICAM system.
15. Software version control and Defect tracking software will be provided by the State for this project.
16. The State will provide participants fully knowledgeable in the State's policies and procedures for employees, contractors, vendors, job functions, job changes, new hires, termination, leave, reporting, audit, and compliance.
17. The State will supply necessary sample data to be used to populate the non-production environments and to provide test data that represents production data. It is assumed that the data provided to Contractor will be free of any personally identifiable information (PII) or other sensitive data.
18. Contractor will use the IBM IAM suite of products for implementing MICAM solution. As the State has an IBM Tivoli solution integrated with a number of existing applications, we have assumed that the State will provide/share the source code for existing connectors (OOTB or custom) along with any customizations (e.g. workflows, notifications etc.) that will be re-purposed/re-used with the new MICAM solution.
19. At project initiation the supporting documentation from the existing IBM Tivoli, NetIQ, and Microsoft Forefront based IAM implementations to be provided to the project team. Required documentation includes, but is not limited to:
 - Technical design documentation
 - Use case documentation
 - Workflow documentation
 - Data flow documentation
 - Configuration documentation
20. There are known limitations with IBM products as identified in the Voluntary Product Accessibility Templates (VPAT). Should a situation where the State's accessibility requirements are not met due to product limitations, we will work with the State to perform an impact analysis. Contractor will present the limitations and findings to the State and cooperate with the State, IBM and the State's external accessibility testing vendor in their efforts to find an acceptable alternative for the specific, inaccessible feature. However, Contractor is not responsible for the implementation and/or customization required for these acceptable alternatives.
21. Rollout of functionality may require system/component downtime in a given MICAM environment, including the MICAM production environment. Contractor will coordinate with the State to determine the downtime requirements and coordinate rollout of these MICAM project phases and threads.
22. In order to enable Federation SSO, the configuration changes will be required on both MICAM and other Identity and Access Management system (e.g. IAM for MIHIN for the application identified for Federation pilot) to enable and configure Identity federation, i.e., Federation SSO. Contractor will only be responsible for configuration changes on the MICAM solution. The State staff will be responsible for configuration changes on the other IAM systems and applications to enable Federation with MICAM solution.



23. For purposes of this project, the terms “audit” and “auditing” refer to the implemented system’s ability to track and record specified activities in a log or repository. It does not refer to any third-party recommendation on the capability of the design.
24. For the purpose of this project, the terminology IBM Tivoli and IBM Security are used inter-changeably as IBM has rebranded the IBM Tivoli products to IBM Security in newer releases.
25. Contractor’s scope does not include fixes to any pre-existing defects in integrated applications, existing infrastructure, and supporting components.
26. For planning purposes, we have assumed that the Contractor’s Applications Management Process Manager (AM-PM) service management tool will be leveraged as a help desk ticketing system for the MICAM solution. Also, any Service Level Agreement (SLA) determined during project negotiation will be applicable from the point a formal ticket is submitted through this AM-PM System.
27. For planning purposes, we have assumed the following hours of service for Help desk and Ongoing support activities
 - Hosted Platform Support : 24*7, 365 days/year
 - MICAM Solution Support: 8*5 with on call support for out of office hours and on weekend
28. IBM Security Access manager for e-Business (SAM) will only provide coarse grained authorization for the applications in-scope of this project.
29. The State of Michigan will upgrade the target’s software version (applications and related infrastructure components) if that is required to allow for OOTB integration with the MICAM solution components.
30. Contractor is not responsible for any data cleansing associated with the proposed MICAM solution. Contractor is not responsible for confirming the proper data integrity and consistency of information extracted from the current systems and managed applications and platforms.
31. For cost section, the cost specified in Table 5, i.e., Help desk cost, is based on the State of Michigan’s response during the RFP Question and Answers with respect to this RFP for the expected call volumes. However, during the monthly status reviews, both Contractor and State of Michigan will get an opportunity to review actual demand versus estimates and make recommendations for appropriate changes to Help Desk staffing requirements. Any change identified will be addressed through a change request.
32. For planning purposes, we have considered that the Help desk support will be provided in English and Spanish only. If it is determined by the State of Michigan that Help desk support is also required in additional languages, then it will be addressed through a change request.
33. For cost section, the cost specified in Table 6, i.e., Migrations of Existing SSO Applications Costs, considers the following
 - a. Maximum one hundred ninety-five (195) applications to be migrated to MICAM (as specified in MICAM Appendix C Migration and Integration Types) from month 7 – 36 of the project. For planning purposes, we have considered the following number or less of applications to be migrated from the existing IBM Tivoli, NetIQ, and Microsoft Forefront IDM based solutions.
 - i Existing IBM Tivoli based solution = 125 applications
 - ii Existing NetIQ based solution = 35 applications
 - iii Existing Microsoft Forefront IDM based solution = 35 applications
 - b. Migration of application from month 7 – 24 of the project.
 - i Month 7 - 12: 50 Tivoli based applications (Type A = 2, B = 2, C = 40, D = 2, E = 4)
 - ii Month 13 - 18: 50 Tivoli based applications (Type A = 3, B = 3, C = 40, D = 3, E = 1)
 - iii Month 19 - 24: 25 Tivoli based applications (Type A = 1, B = 1, C = 20, D = 1, E = 2)



- iv Month 25 - 30: 35 NetIQ based applications (Type A = 2, B = 2, C = 25, D = 2, E = 4)
 - v Month 31 - 36: 35 Microsoft Forefront IDM based applications (Type A = 2, B = 2, C = 25, D = 2, E = 4)
- c. The estimated cost is determined by using the estimated hours for different application types provided by the State of Michigan. However, before migration of applications as indicated in 48.b.i – 48.b.v above, these estimates will be reviewed for effort and cost. As applicable, the deviation in initially provided estimates and those determined during planning of every three (3) months, before the migration of applications, will be addressed through a change request (CR).
34. For cost section, the cost specified in Table 7, i.e., Operational Services Costs for New Integrations, considers the following:
- a. Maximum two hundred (200) new applications to be integrated with MICAM (*as specified in MICAM Appendix C Migration and Integration Types*) from month 19 – 60 of the project. For planning purposes, we have considered the following number or less of applications to be integrated with the proposed MICAM solution.
 - i Month 19 - 24: 25 applications (Type A = 5, B = 5, C = 5, D = 4, E = 4, F = 1, G = 1)
 - ii Month 25 - 30: 15 applications (Type A = 3, B = 3, C = 3, D = 2, E = 2, F = 1, G = 1)
 - iii Month 31 - 36: 15 applications (Type A = 3, B = 3, C = 3, D = 2, E = 2, F = 1, G = 1)
 - iv Month 37 - 42: 35 applications (Type A = 6, B = 6, C = 7, D = 7, E = 6, F = 0, G = 3)
 - v Month 43 - 48: 35 applications (Type A = 7, B = 7, C = 6, D = 6, E = 7, F = 2, G = 0)
 - vi Month 49 - 54: 35 applications (Type A = 6, B = 6, C = 7, D = 7, E = 6, F = 0, G = 3)
 - vii Month 55 - 60: 40 applications (Type A = 7, B = 7, C = 7, D = 7, E = 7, F = 2, G = 3)
 - b. The estimated cost is determined by using the estimated hours for different application types provided by the State of Michigan. However, before onboarding new applications as indicated in 49.a.i – 49.a.vii above, these estimates will be reviewed for effort and cost. As applicable, the deviation in initially provided estimates and those determined during planning of every three (3) months, before the onboarding of new applications, will be addressed through a change request (CR).
35. For planning purposes, we have considered total three (3) sessions of four (4) hours each in every three (3) month period for training the staff identified by the State of Michigan for conducting the User Acceptance Testing (UAT) of the MICAM solution. It is the State of Michigan’s responsibility to coordinate with its staff to make them available for these training sessions. These training will be focused on the MICAM solution to enable State of Michigan staff to perform UAT and does not include product related trainings. Contractor may provide additional MICAM solution training, IAM product training, or transition services, at the request of the State of Michigan, upon execution of a change request for these activities.
36. The cost for IBM Tivoli Identity and Access Management (IAM) software specified in Cost section - Table 8, i.e., Licensing cost, considers that six (6) IBM Tivoli Federated Identity Manager Business Gateway (TFIM BG). The TFIM BG will be leveraged for Risk-Based Authentication (RBA) and depending on the number of applications, total users, and concurrent users requiring this capability the sizing will be reviewed for capacity and performance during the planning exercise, before integration of applications identified by the State of Michigan. As applicable, the deviation in initially provided sizing and those determined during planning, before the integration of applications, will be addressed through a change request (CR).
37. For cost section, the estimation of hours by resource for Table 10, i.e., Reserved Bank of Hours for Future Projects Costs, is provided as a high level budgetary estimate as the scope and requirements are unknown at this time. Once we review the detailed scope and requirements for the work identified by the State of Michigan for “Future Projects” we will provide detailed estimates and staff leverage model to accomplish the tasks and deliverables. Any scope and/or budget impact for “Reserved Bank of Hours for Future Projects Costs” will be managed through a change request.



38. Any references to out-of-the-box or standard functionality provided by IBM and its IAM software refers to standard provided functionality within the product being referenced. For the purposes of this proposal, the following IBM functionality is considered out-of-the-box:
- Configuration of the IBM product via its native configuration screens
 - Configuration of out-of-the-box IAM connectors for all ISIM integrations
 - Configuration of pre-built reports provided by IBM for Security Identity Manager (ISIM) and Security Access Manager for e-Business (ISAM)
 - Configuration of ISAM and WebSEAL for authentication and coarse authorization
- Any other types of modifications to ISIM, ISAM, IBM Tivoli Federated Identity Manager (TFIM), IBM Tivoli Directory Integrator (TDI), IBM Tivoli Directory Server (TDS), IBM DB2, or IBM DataPower are considered out of scope for Contractor's services unless otherwise noted in this proposal.
39. For planning purposes, we have assumed that phase 2, i.e., migration of existing applications, will only include the "As-Is functionality" migration of applications to the proposed MICAM solution. The proposed fee does not include any new functional or non-functional requirements to be added during the migration of applications to the proposed MICAM solution. If required by the State of Michigan, new functional and non-functional requirements will be addressed through the change request.
40. It is assumed that the State's Active Directory (AD) Forests and Domains that will be leveraged for integration with ISAM has trust enabled between various AD forests and Domains.
41. It is assumed that the userPrincipalName attribute of the State's Active Directory instance uses the default format. ISAM does not support using alternate user principal name (UPN) format with SPNEGO authentication. The default format for the userPrincipalName attribute in Active Directory is user_shortname@domain, where "domain" is the Active Directory domain in which the user was created. Tivoli Access Manager SPNEGO authentication only supports the default format of the userPrincipalName attribute as the Active Directory user identity.
42. State will provide performance monitoring tools for the State hosted MICAM solution.
43. Contractor may utilize software that is currently owned by or licensed to Contractor in connection with the performance of its services. If the State would like Contractor to use other software, such software is to be acquired by and licensed to the State, with Contractor as a sub licensee for use in connection with the performance of its services to the Company at no cost to Contractor. With respect to software that is owned or licensed to Contractor, if the State personnel will access or use such software, the State agrees to become a licensee in accordance with terms established by Contractor.



State of Michigan
Administrative Guide to State Government

POLICY 1340.00 Information Technology Information Security

Issued: April 12, 2007

Revised: March 21, 2012

SUBJECT: Policy for Information Technology (IT) Information Security.

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

PURPOSE: This policy establishes the SOM executive management strategic view of how information security shall be implemented to protect the SOM information from unauthorized access, use, disclosure, modification, destruction, or denial and to ensure confidentiality, integrity and availability of SOM information.

CONTACT AGENCY: Department of Technology, Management and Budget (DTMB)
Michigan Cyber Security

TELEPHONE: 517-241-4090

FAX: 517-241-2013

SUMMARY: All SOM employees, trusted partners, or any entity authorized to access the SOM information is obligated to 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 contained in computer systems but is inclusive regardless of where it resides within the agency, what form it takes, (*i.e.*, electronic, printed, etc.), what technology was used to handle it, or what purpose(s) it serves. This policy is based on three basic components of information Security for the purpose of this policy:

- **Confidentiality** – Limiting information access and disclosure to authorized users – “the right people” – and preventing access by or disclosure to unauthorized users – “the wrong people.” Confidentiality is defined as protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.
- **Integrity** – The trustworthiness of information resources. It includes the concept of “data integrity” – namely, that data have not been changed inappropriately, whether by accident or deliberate activity. It also includes the need to verify that the person or entity has entered the right information – that is, that the information reflects the actual circumstances and that under the same circumstances would generate identical data. Integrity is defined as guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose.
- **Availability** – The availability of information resources. An information system that is not available when you need it is at least as bad as none at all. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure. Availability is defined as ensuring timely and reliable



access to and use of information and assuring that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Based on these three components of information security, any data that is originated, entered, processed, transmitted, stored or disposed of on behalf of the SOM is considered to be SOM information.

POLICY:

- Agency information is considered a SOM asset and must be appropriately evaluated and protected against all forms of unauthorized access, use, disclosure, modification, destruction, or denial.
- Each agency Director is required to determine the proper levels of protection for their agency information and to implement the necessary safeguards.

Agency Director:

- As a Data Owner, the Director within their area of responsibility shall ensure:
 - Due diligence of confidentiality, integrity and availability of data.
 - Data management in compliance with Federal and state laws and regulations, and SOM policies.
 - Information security controls are implemented to protect the SOM information and that these controls are sufficient to ensure the confidentiality, integrity, availability of SOM information.
 - Information security controls are applied in a manner consistent with the value of the information.
 - Data business owner identification. Although it is not recommended to have multiple owners for the same data, this sometimes occurs. Where there is more than one owner, Data Owners must designate a Business Owner who will have authority to make decisions on behalf of all the owners of this data.
 - SOM agency information is identified and classified based on sensitivity, criticality and risk in compliance to Federal and state laws and regulations, includes a review at least once a year of the on-going need to continue protection, updates when the environment changes.
 - A system is established to identify baseline security controls to protect SOM information. Once it is identified and classified, ensure it is exposed only to those who have a need to know the information and a duty to protect it.
 - SOM agency information is safeguarded with the proper controls in accordance with its classification label.
 - Data, which is shared or transferred between agencies, is protected by the receiving agency with at least the same level of security used by the sending agency. The receiving agency assumes the responsibility of data owner for such data when it is transferred.
 - Anyone requiring access to confidential or restricted information that is owned by another agency must obtain permission from the Business Owner.
 - Controls are established to provide SOM oversight of trusted partners who handle SOM information on behalf of the SOM.
 - SOM agency information is disposed of and sanitized in compliance with SOM policies.
 - A formal internal process is established for reporting and responding to security breaches/incidents where there is reasonable belief that an unauthorized person may have acquired personal identifying information.



- o A system is established to review technical controls and recommendations identified by the SOM data custodians.
- o Internal agency security policies and procedures are implemented, maintained and enforced that compliment and comply with this policy.
- o All SOM employees and trusted partners handle information for which they are responsible in compliance with this policy and all SOM IT policies.
- o SOM employees and trusted partners are trained to ensure they are aware of their role in protecting SOM information and data as set forth in this policy.
- o Employees are advised of the necessity of complying with DTMB policies and laws pertaining to the protection of SOM information, because non-compliance may leave the state liable and employees vulnerable to prosecution and civil suite, as well as disciplinary action.

DTMB Director:

- As a Data Custodian, the Director shall ensure:
 - o Agencies are advised as to the best operational and technical controls necessary to protect their data in accordance with its classification label.
 - o Agency-prescribed security controls and safeguards are implemented and monitored for compliance.

Terms and Definitions:

Agency	The principal department of state government as created by Executive Organization Act, P.A. 380 of 1965.
Availability	Ensuring timely and reliable access to and use of information and assuring that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.
Business Owner	Responsible for administration of systems is usually the owner of the primary business functions served by the application, the application's largest stakeholder.
Confidentiality	Protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.
Data Custodian	An individual or organization that has responsibility delegated by a data owner for maintenance and technological management of data and systems.
Data/Information	SOM agency information. No distinctions between the words data and information are made for purposes of this policy.
Data Owner	An individual or organization – usually a member of senior management of an organization – who is ultimately responsible for ensuring the protection and use of data.
Due Care	Shows that an organization has taken responsibility for the activities that take place within the organization and has taken the necessary steps to help protect the SOM, its resources and employees from possible risk.
Due Diligence	The practice of implementing controls and safeguards that make sure the protection mechanisms are continually maintained and operational.



Information Technology (IT) Resources	Includes, but is not limited to: computers, servers, storage peripherals, telecommunications equipment, network equipment and wiring, network-attached printers and fax machines.
Integrity	Guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose.
Technical Policy(ies)	High-level executive management statements used to set directions in an organization that documents information values, protection responsibilities and management commitment for protecting its computing and information assets. Policies are strategic in nature.
Technical Standards	Published documents that contain technical specifications or other precise criteria designed to be used consistently as a rule, guideline or definition. They are also a collage of best practices and business cases specific to address an organization's technological needs. Standards are tactical in nature and derive their authority from a policy.
Technical Procedures	A series of prescribed steps followed in a definite order which ensure adherence to the standards and compliance as set forth in the Policy to which the Procedure applies. Procedures are operational in nature and derive their guidance from a standard and authority from a policy.
Trusted Partner/ Business Partner	A person (<i>i.e.</i> , vendor, contractor, 3rd party, etc.) or entity that has contracted with the SOM to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, or goods and services.

Authority:

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

Enforcement:

- All enforcement for this policy shall be in compliance 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 shall be in compliance 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 will be effective upon signature of the Administrative Guide approval memo by the DTMB Director.



POLICY 1310 Information Standards and Planning

Issued January 6, 1997

Information Standards

Executive Branch Departments and Sub-Units shall obtain approval to acquire information processing studies, consultation contracts, resources and systems; design, implement and maintain automated information processing systems, installations and services; pay for the cost of these services, and report expenditures for State automated information processing systems, services and resources, all in conformance with DTMB procedures and directives.

The purpose of the State telecommunication network is to facilitate information exchange in support of state government functions. These resources and value-added services are primarily intended to assist state employees in the performance of their assigned state government tasks. The State reserves the right to monitor and log all network activity, including E-mail, with or without notice, and therefore users should have no expectation of privacy in the use of these resources.

Use of the state telecommunication infrastructure is a revocable privilege, requiring compliance and conformity with this acceptable use policy. Agencies must enforce this policy and inform their employees and contractors of this policy. Contractors who need and are granted access by the agency to the State network, are restricted to only those resources necessary to accomplish their contractual, legal or administratively assigned state government task.

The Management and Budget Act, Public Act 431 of 1984, as amended, ' 203 Section 18.1203 of Public Act 431 of 1984 as amended Executive Order Number 1994-15 (Statewide Telecommunications Consolidation) dated May 21, 1994.

* * *



1310.02 Information Processing Security

Issued: January 1, 1994

SUBJECT: Information Processing Security.

APPLICATION: Executive Branch Departments and Sub-units.

PURPOSE: To provide the procedures to secure and protect State information processing facilities, data and media, software, hardware and personnel.

CONTACT AGENCY: Department of Technology, Management and Budget (DTMB)
Bureau of Research and Policy

TELEPHONE: 517/373-7326

FAX: 517/335-2355

SUMMARY: The procedures are designed to cover all pertinent responsibilities that relate to information processing security. Because of this, certain guidelines are not the direct responsibility of the information processing manager and may require coordination with other external agencies.

APPLICABLE FORMS: As required.

PROCEDURES:

Instruction A: Mainframe and General Information Processing

Agency insures that:

- Physical site:
 - In a multi-storied building, the computer room must be located above the first floor (applies to newly constructed computer rooms only).
 - A computer room will not be located adjacent to exterior walls or near building entrances (applies to newly constructed computer rooms only).
 - Fire resistant walls, ceiling, doors, and flooring must surround the computer room. Computer room walls must not contain windows if they are part of the building exterior (applies to newly constructed computer rooms only).
 - In multi-storied buildings, the floor above the computer room must be made water tight (applies to newly constructed computer rooms only).
 - The computer room must be equipped with smoke and heat detectors as determined by the appropriate fire regulations.
 - Remote switches, other than the actual machine on/off switches to shut off all installation power, must be installed near the entrance or exit of the computer room.
 - Approved portable extinguisher, per Fire Marshal specifications, must be available and clearly marked.
 - Emergency lighting is mandatory.

Procedure Update: 05/01/01

Procedure 1310.02

Page -1-



- All equipment that requires grounding must be grounded.
- Walls must extend from structural floor to structural ceiling in computer room where room construction features permit.
- Drains must be installed under raised floors and water detectors must be used (applies to newly constructed computer rooms only).
- Entrance and exit doors must remain locked and equipped with alarms.
- Raised floor panel lifters must be available.
- Fire and smoke detectors, fire extinguisher, alarms, emergency exits, and alternative power supplies must be tested and maintained.
- Evacuation route floor plans must be posted in conspicuous locations.
- Circuit breaker panels must be located in a secure area and their locations marked.
- Manually operated alarm locations must be easily accessible and conveniently located.
- Define and document how and who Building Management must notify in case of any scheduled or emergency interruption in service for the following:
 - Electrical power
 - Water service
 - Environment
 - Drainage service
- Each data center must develop and issue procedures for emergency interruptions in service and make periodic tests to ensure that the procedures are effective.
- Written procedures to provide a secure computer room must include:
 - Who is authorized in the computer room during prime and non-prime shifts and how are they to be recognized and admitted.
 - Restrictions on eating, drinking, and smoking in the computer room.
- All guided tours of the information processing facility must be pre-scheduled. No unguided tours will be conducted.
- Environmental conditions must be defined and documented for the computer room as must the person who is responsible for monitoring them.
- The primary file library area must be designed as a restricted area and must not have windows or public access.
- An off-site back-up file library or vault must be utilized which is a minimum of 5 miles from the main processing site.
- If a vault is used for security, the vaults must remain closed and locked except when materials are being removed or placed in vaults.



- Each department must designate a primary and secondary location for all production systems documentation to include back-up copies of operation guides.
- Written procedures must exist for original issues as well as lost stolen, or forgotten keys, cards, and badges used to access the computer room.
- Software controls:
 - Terminals must not display passwords when keyed.
 - System software must protect passwords or other security information.
 - Security violations must be logged.
 - Security violation log must be reviewed and problems resolved.
 - Terminals must be automatically logged off after repeated attempts to gain access or if left unattended for a specific period of time.
 - Procedures must be established and implemented for controlling dial-in access to a computer system.
 - Production program and data files must be protected against unauthorized access.
 - Telecommunications software must generate terminal usage reports to data center management.
 - Passwords must be assigned in a secure manner, periodically changed, and promptly deleted for terminated employees.
 - Security requirements and procedures must be documented and approved by management for each application system.
 - Procedures must be established and implemented for monitoring computer console (ODT) activities for the purpose of identifying security and procedural violations.
 - Procedures must be established and implemented for scheduling all jobs through the computer system. Special requests must be authorized before the job is run.
 - Execution reports or other reports must be reviewed to ensure jobs are run correctly.
 - A written request must be given to the appropriate organizational unit prior to modifying production programs.
 - Data center management must require all system software changes to be documented and approved.
 - System utilities, which override or bypass controls, must not be used unless approved by data center management.

Procedure Update: 05/01/01

Procedure 1310.02

Page -3-



- **Data and media:**
 - All master and transaction files (necessary for update of master files) must have at least one back-up file. If feasible, 2 back-up files should be available. (A back-up file may be a duplicate file, first or second generation file.)
 - Written procedures must be established for the file librarian and must contain the following:
 - Physical security procedures.
 - Who is authorized and channels through which files can be released.
 - Log in and out procedures for all files going outside the installation.
 - Back-up file procedures.
 - Emergency interruption of service procedures.
 - Person who knows the safe combination.
 - Retention cycle procedures.
 - Each production file must have a unique, approved file identification (ID) number on the gummed label and on the header label. This unique ID number must begin with a 1-digit State department code, thus eliminating any duplicate ID numbers.
 - Each tape and removable disk must have an assigned serial number.
 - Tape containers, seals, or pack containers must be used during all non-machine processing periods.
 - File protect rings must be removed from all tape files to be saved.
 - Confidential reports must be labeled as being confidential or containing proprietary information and must remain in a secure area until picked up by an authorized user.
- **Personnel:**
 - An individual must be designated as the security officer for each site or installation.
 - A security check must be made on all new personnel hired to work in a data center prior to employment.
 - Computer operations functions must be organizationally separated from computer operations and applications programming functions.
- **Miscellaneous:**
 - Authorized signatures must be required when releasing confidential information.
 - All contracts involving outside contractors must contain a security clause if the contractor is to have access to confidential data and/or to the data center itself.

Procedure 1310.02

Procedure Update: 05/01/01

Page -4-



- Erroneously created confidential information must be shredded or otherwise destroyed.
- Confidential documents, forms, and negotiable documents must be stored, controlled, and periodically inventoried.

Instruction B: End-user Computing (EUC) Security

All departments and agencies shall have the responsibility for managing the security of resources associated with End User Computing (EUC).

- General:

Internal policies and procedures must be developed to address the following EUC security issues:

- An individual must be designated as EUC Security Officer with responsibility for:
 - Implementing and enforcing security policies and procedures.
 - Regularly reviewing EUC security effectiveness.
 - Reviewing and recommending to data center management any changes to EUC security policy and procedure.
- Ensuring the compatibility and consistency with other data center and departmental policies and procedures.
- Performing regular (and random) site inspections and user reviews to verify:
 - Physical inventories.
 - Environmental conditions.
 - General compliance with EUC policies and procedures.
 - Training and communications (to ensure awareness of EUC policies as well as operational information).
 - Service request process (to track and prioritize needs and problems associated with EUC).

- Physical Security:

Internal policies and procedures must be developed to address the following physical security issues:

- Central identification and inventory of all hardware, including regular and random physical inventory checks.
- Location and movement of any and all EUC equipment.
- Connection or disconnection of any and all EUC equipment.
- Site and environment requirements or restrictions.
- Maintenance and service.

Procedure Update: 05/01/01

Procedure 1310.02

Page -5-



- Identifications of all valid users and conditions of access.
- Media protection procedures with specific concern for hard disk storage units.
- **Software Security:**
Internal policies and procedures must be developed to address the following software security issues:
 - Identification and periodic review of any and all license agreements associated with all software.
 - Informing and training users of their responsibility regarding license restrictions and software usage (e.g., copy restrictions).
 - Central identification and inventory of all software authorized to be used and supported on EUC equipment.
 - Internal software development policy (procedures to describe any and all restrictions to be placed on internally developed application software including programming standards, languages and support).
 - Support and assistance procedures.
- **Data Security:**
Internal policies and procedures must be developed to address the following data security issues:
 - Identification of data owners.
 - Data maintenance and release (data owners define the procedures for use by others).
 - Documentation, backup, and recovery procedures.
 - Local data vs. inter divisional or departmental data.
 - Confidential or sensitive data.
- **Networks:**
Internal policies and procedures must be developed to address the following:
 - Standards and conditions for any and all local area network hardware and software.
 - Standards and conditions for any and all in-house mainframe connections.
 - Access to external networks and mainframes.
 - Communications software.
 - Installation and access to modems and data communications lines



State of Michigan
Administrative Guide to State Government

POLICY 1335 Information Technology Access Control

Issued: April 12, 2007

Revised: March 21, 2012

- SUBJECT:** Policy for Information Technology (IT) Access Control.
- APPLICATION:** This policy is intended for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, Boards or Commissions using state of Michigan (SOM) information networks and IT resources.
- PURPOSE:** This policy establishes the SOM executive management strategic view of how employees and trusted partners shall obtain access to established services on the SOM network. This policy further establishes the protection of information and systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users. Such access must be controlled with secure means of authentication, authorization and accountability.
- This policy focus is on users obtaining access to established SOM services. If a service does not exist, the Administrative Guide Policy 1345 Information Technology Network & Infrastructure will direct you to compliance in establishing a new SOM services.
- CONTACT AGENCY:** Department of Technology, Management and Budget (DTMB)
Michigan Cyber Security
- TELEPHONE:** 517-241-4090
- FAX:** 517-241-2013
- SUMMARY:** **Access Control** is the protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities.
- Access to the SOM network and IT resources and other technology resources shall be strictly controlled such that only SOM authorized users have access to the available information.
- This policy will define the access controls required prior to users and systems gaining access to the SOM network and IT resources, controlling the actions they can take and track what action was taken on the resources the user has accessed. This policy is based on three basic components of access control and they are defined as:
- **Authentication** – The process of determining whether someone or something (system) is, in fact, who or what it is declared to be. Example: use of a password to confirm correct association with a user name or account name.
 - **Authorization** – The process of giving the authenticated person or system access to the SOM network and IT resources and determining what type of access is allowed, (e.g., read-only, create, delete, and/or modify).
 - **Accountability** – The process of determining the identity, activity and usage of a system by a user or system.



POLICY:

- It is the agency/department who gathers data, enters it into the system, verifies its accuracy, specifies the purposes to which it can or will be used, designates who can use it, and ultimately fills a business need for its use.

Agency Director:

- As a Data Owner, the Director within their area of responsibility shall ensure:
 - A formalized process is developed to manage user access to the SOM Network and IT resources in compliance with this and all SOM policies that:
 - Limits access to authorized users whose job responsibilities require it as determined by the agency internal approval process.
 - Allows access to be managed, controlled and periodically reviewed and audited to ensure user access is based on specific privilege granted.
 - Provides a mechanism for controlling and documenting the allocation of user access rights from initial access rights, as a new user, through to de-registration, when the user changes jobs or leaves the agency.
 - Utilizes methods that provide user authentication, authorization and accountability.
 - Promotes separation of duties, least privilege and a need to know.
 - Ensures users approved to access established services on the SOM network and IT resources are approved in compliance with this and all SOM policies.
 - Internal agency security policies and procedures are implemented, maintained and enforced that compliment and comply with this policy.
 - State departments desiring to implement more stringent policies than those developed by DTMB, may do so in conjunction with DTMB.

DTMB Director:

- As a Data Custodian, the Director shall ensure:
 - All agencies have access to the SOM policies, standards, procedures and guidelines governing user access to the SOM network and IT resources.
 - A formal process is established to manage user access to the SOM network and IT resources (LAN, WAN, file and print, desktop, etc.).
 - A formal process is established to implement and audit agency approved access requests to established services, (i.e., wireless, Telecom catalog services, application access, new employee access, etc.) on the SOM network in compliance with this and all SOM policies.
 - A formal process is established that ensures the proper implementation and integration of service continuity with other system operations and technical security controls as prescribed by DTMB in conjunction with the agencies.

Terms and Definitions:

Agency	The principal department of state government as created by Executive Organization Act, P.A. 380 of 1965.
Availability	Ensuring timely and reliable access to and use of information and assuring that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.



Business Owner	Responsible for administration of systems is usually the owner of the primary business functions served by the application, the application's largest stakeholder.
Confidentiality	Protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.
Data Custodian	An individual or organization that has responsibility delegated by a data owner for maintenance and technological management of data and systems.
Data/Information	SOM agency information. No distinctions between the words data and information are made for purposes of this policy.
Data Owner	An individual or organization – usually a member of senior management of an organization – who is ultimately responsible for ensuring the protection and use of data.
Due Care	Shows that an organization has taken responsibility for the activities that take place within the organization and has taken the necessary steps to help protect the SOM, its resources and employees from possible risk.
Due Diligence	The practice of implementing controls and safeguards that make sure the protection mechanisms are continually maintained and operational.
Information Technology (IT) Resources	Includes, but is not limited to: computers, servers, storage peripherals, telecommunications equipment, network equipment and wiring, network-attached printers and fax machines.
Integrity	Guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose.
Trusted Partner/ Business Partner	A person (<i>i.e.</i> , vendor, contractor, 3rd party, etc.) or entity that has contracted with the SOM to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, or goods and services.

Authority:

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

Enforcement:

- All enforcement for this policy shall be in compliance 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 shall be in compliance 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 will be effective upon signature of the Administrative Guide approval memo by the DTMB Director.



State of Michigan
Administrative Guide to State Government

POLICY 1325 Information Technology Security Awareness

Issued: April 12, 2007

Revised: March 21, 2012

- SUBJECT:** Policy for Information Technology (IT) Security Awareness.
- APPLICATION:** This policy is intended for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, Boards or Commissions using state of Michigan (SOM) information networks and IT resources.
- PURPOSE:** This policy establishes a statewide policy for the purpose of security awareness and training and to inform all levels of state personnel of the importance of the information they handle and the legal and business reasons for maintaining confidentiality, availability and integrity. All employees must understand the need for security, the specific security-related requirements expected of them, and the consequences of noncompliance.
- CONTACT AGENCY:** Department of Technology, Management and Budget (DTMB)
Michigan Cyber Security
- TELEPHONE:** 517-241-4090
- FAX:** 517-241-2013
- SUMMARY:** This policy will address two major security awareness components:
- **Awareness (What)** – Identify and implement programs and products designed to convey general security information to SOM users. Such activities include, but are not limited to, a statewide information security awareness training program, generating security literature and promoting good security through security web sites and newsletters.
 - **Training (How)** – Identify and implement security training programs more specific to the user role (*i.e.*, project manager, system administrator, security liaison, etc.) within the agency. This will provide the users with training applicable to their level of responsibility.

POLICY:

- It is the agency/department who gathers data, enters it into the system, verifies its accuracy, specifies the purposes to which it can or will be used, designates who can use it, and ultimately fills a business need for its use.

Agency Director:

- As a Data Owner, the Director within their area of responsibility shall ensure:
 - The appointment of a security awareness coordinator who will serve as liaison to the DTMB security awareness coordinator.
 - All SOM employees and trusted partners complete the SOM Information Security Awareness training prior to accessing the SOM network and IT resources.
 - All SOM employees and trusted partners handle information for which they are responsible in a manner in accordance with this and all SOM policies.
 - SOM employees and trusted partners are trained to ensure they are aware of their role in protecting SOM information and data as set forth in this policy.



- o Internal agency security policies and procedures are implemented, maintained and enforced that compliment and comply with this policy.
- o Employees are advised of the necessity of complying with DTMB policies and laws pertaining to the protection of SOM information, because non-compliance may leave the state liable and employees vulnerable to prosecution and civil suit, as well as disciplinary action.
- As a Data Custodian, in conjunction with the DTMB Chief Information Security Officer (CISO) shall ensure:
 - o A structured SOM security awareness program is formulated and maintained to ensure that SOM employees and trusted partners who require access to the state's information in the conduct of official business are familiar with their responsibilities for protecting such information from unauthorized disclosure.
 - o All agencies implement security awareness workshops for agency security awareness coordinators.

DTMB CISO:

- Shall ensure:
 - o A security awareness coordinator is appointed to develop and implement an enterprise security awareness program.

Terms and Definitions:

Agency	The principal department of state government as created by Executive Organization Act, P.A. 380 of 1965.
Availability	Ensuring timely and reliable access to and use of information and assuring that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.
Business Owner	Responsible for administration of systems is usually the owner of the primary business functions served by the application, the application's largest stakeholder.
Confidentiality	Protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.
Data Custodian	An individual or organization that has responsibility delegated by a data owner for maintenance and technological management of data and systems.
Data/Information	SOM agency information. No distinctions between the words data and information are made for purposes of this policy.
Data Owner	An individual or organization – usually a member of senior management of an organization – who is ultimately responsible for ensuring the protection and use of data.
Due Care	Shows that an organization has taken responsibility for the activities that take place within the organization and has taken the necessary steps to help protect the SOM, its resources and employees from possible risk.
Due Diligence	The practice of implementing controls and safeguards that make sure the protection mechanisms are continually maintained and operational.



Information Technology (IT) Resources	Includes, but is not limited to: computers, servers, storage peripherals, telecommunications equipment, network equipment and wiring, network-attached printers and fax machines.
Integrity	Guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose.
Trusted Partner/ Business Partner	A person (<i>i.e.</i> , vendor, contractor, 3rd party, etc.) or entity that has contracted with the SOM to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, or goods and services.

Authority:

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

Enforcement:

- All enforcement for this policy shall be in compliance 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 shall be in compliance 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 will be effective upon signature of the Administrative Guide approval memo by the DTMB Director.



**1350.10 Authentication Requirement for Access to Networks, Systems, Computers,
Databases, and Applications**
Issue Date: August 18, 2006

- SUBJECT:** Authentication Requirement for Access to Networks, Systems, Computers, Databases, and Applications.
- APPLICATION:** This procedure applies to all Executive Branch Departments, Agencies, Boards or Commissions using State information technology resources including, but not limited to, networks, systems, computers, databases, and applications.
- This procedure does not apply to general public access to public or open information presented in HTML, voice, video, TTD, or other web compatible formats over the Internet or through the public switched telephone network.
- PURPOSE:** This procedure requires the identification and use of approved personal authentication methods, appropriate for the identified level of security required, for access to State of Michigan information technology resources to prevent unauthorized access or maintain resource data integrity.
- CONTACT AGENCY:** Department of Technology, Management and Budget (DTMB)
Office of Enterprise Security
- TELEPHONE:** 517/241-4090
- FAX:** 517/241-2013
- SUMMARY:** This procedure requires that State agencies, using the risk and severity profile analysis defined in Procedure 1350.50, identify the level of risk and severity of any associated loss of data for all Agency information technology resources. DTMB, in coordination with the Agency, will identify and implement the appropriate method and level of authentication needed to safeguard each identified resource from unauthorized access.

APPLICABLE FORMS: None

PROCEDURES:

- A. The use of an appropriate and approved method of personal authentication is required for access to all State information technology resources.
- B. All users authorized to access State information technology resources must provide authentication of authorized access at each access level identified in conformance with this procedure or as otherwise approved in writing by the DTMB Office of Enterprise Security. Authentication must be provided whether the point of access is from within the State's systems or from a connection point external to the State.
- C. **Agency responsibilities:**
 1. Each Agency must identify the level(s) of personal authentication required for Agency-specific information technology resources.
 - a. Agencies must use the risk and severity profile defined in Procedure 1350.50, Web Application Risk Assessment Framework for the Use of PKI Certificates, and select the profile best associated with the resource:
 - i. Risk zero, Severity zero - Public and FOIA-able information;
 - a. No authentication required,

Issue Date: 08/18/06

Procedure 1350.10

Page -1-



- b. At this level, zero confidence in the identity of the end-user is needed.
 - ii. Risk one, Severity one - Protected information, system, or application;
 - a. User id & password authentication,
 - b. At this level, moderate confidence is needed that the end-user identity is valid.
 - iii. Risk one, Severity two - Protected information;
 - a. Two-factor authentication or approved business process,
 - b. A high confidence is required of the end-user's identity.
 - iv. Risk two, Severity one - Protected information;
 - a. Two-factor authentication,
 - b. A high confidence is required of the end-user's identity.
 - v. Risk two, Severity two - Protected information;
 - a. Two-factor authentication and/or password client PKI,
 - b. A very high confidence is required in the end-user's asserted identity.
- 2. Agencies must submit their profile for each information technology resource, in writing, to the DTMB Office of Enterprise Security with a request that the appropriate technical method of authentication matching the risk and severity level be implemented.
 - a. Technical methods of achieving authentication to match the risk and severity level may include:
 - i. User ID and Passwords
 - ii. Biometrics
 - iii. Directories
 - iv. Smart cards
 - v. Single sign-on solutions
 - vi. Tokens
 - vii. PKI & Certificates
 - viii. Voice recognition
 - ix. Shared secrets
 - x. Access control lists and files.
 - xi. Unique business process.

D. DTMB responsibilities:

- 1. The Office of Enterprise Security will refer the profile and request for authentication method to the appropriate technical custodian within DTMB:
 - a. Model Office and Field Services for desktop,
 - b. Agency Services/Application Developers for application authentication,
 - c. Technical Services for Directory/network authentication,
 - d. Telecommunications and Network Management for remote access to network, or
 - e. Technical and Data Center Services for server administration access.
- 2. The technical custodian, in coordination with the Office of Enterprise Security, will:
 - a. Review the written risk and severity profile for compliance with DTMB policies, procedures and standards;
 - b. Determine the appropriate level of authentication, in coordination with the requesting Agency;
 - c. Implement the identified level of authentication, in coordination with the requesting Agency; and
 - d. Certify the fully functioning authentication method has been implemented.
- 3. Office of Enterprise Security will review and monitor authentication controls to ensure appropriate authentication methods are used.
- 4. Internal Auditor shall verify compliance with 1300 and 1400 Series policies and procedures are maintained.

E. State agencies desiring to implement practices and procedures differing from this procedure may do so only with the written approval of the DTMB Office of Enterprise Security.



eMichigan Web Development

Department of Technology, Management & Budget
State of Michigan

Look and Feel Standards for e-Government Applications

Michigan.gov brand elements, policies and information architecture



Version 5.2
April 10, 2013



Table of Contents

About This Document..... 4

Getting Started..... 4

Copyright Information 5

Required Core Branding Elements 6

 Banner Header7

 Sub Header13

 Primary Application Display Area13

 Footer and Policy Links19

Core Policies..... 22

 Security Policy.....22

 Privacy Policy.....23

 Linking Policy23

 Accessibility Policy.....23

Logos and Branding of 3rd Party Applications 24

Copyright..... 25

Screen Resolution 25

Browser Compatibility..... 26

Accessibility and ADA Compliance 28

 Overview28

 Various Disabilities to Consider29

 Font Standards34

 Accessible PDF Documents37

 Common ADA Concerns.....37

 ADA Compliance Testing Tools.....38

Checklist for reviewing applications and websites 40

 Banner 40

 Sub header..... 40

 Main body..... 40



Footer 40

Logos and branding 41

Browser Compatibility 41

Additional Reviews 41

ADA 41



About This Document

Note to all Project Managers and Web Development Teams:

No standards document can take into account every possible combination of web technology. Therefore, it is the responsibility of the IT Project Manager or responsible agent to contact eMichigan Web Development (EWD) to inquire and receive the latest updates and specifications regarding information contained within this document.

This document is intended to communicate important information architecture design and development standards to IT project managers and web design teams. It details the standards and requirements for e-government web sites and applications produced, maintained and operating within the State of Michigan for the purpose of conducting official state business over the World Wide Web or Internet. This includes internal or external facing sites, intended for consumer, business or other government online service audiences.

The intention is to better serve users, whether general citizens or targeted constituents. More importantly, Web Development Teams need to read and understand the information contained within this document. It includes important information about key, required presentation style elements for all State of Michigan online services. These include a consistent and common look and feel across all sites, improved ease of use and overall usability, and reduced time-to-launch through the application of uniform design attributes.

Getting Started

To schedule a review meeting, complete and submit an [Application Review form, DTMB-3533](#)

Based on SUITE project management methodologies and the System Development Life Cycle (SDLC), it is imperative that contact with eMichigan Web Development (EWD) and the Michigan Cyber Security (MCS) be made as soon as possible, preferably at the Initiation Phase of a web based online service solution. Subsequent phases such as Design Requirements will also benefit from this document and review meetings. Review meetings cover a variety of issues ranging from enterprise deliverables, look and feel, policies, security, load testing, usability and pre-launch checklists.

State IT Development Teams, as well as third party development groups contracted or bidding on state IT initiatives, should use these standards as a reference in preparing overall project plans and constructing specific web based applications.



Copyright Information

All aspects of the Michigan.gov brand, either printed or electronic, are under the express control of the Department of Technology, Management & Budget/eMichigan Web Development. Attempts to modify or recreate the Michigan.gov brand image or graphic elements represented within this document are prohibited.

Requests for any Michigan.gov brand element should be made to eMichigan Web Development:

eMichigan Web Development
Department of Technology, Management & Budget
Romney Building – 9th Floor
111 S. Capitol Avenue
Lansing, MI 48913

eMichigan@michigan.gov

This document may be revised as needed to accommodate new standards or revise and edit existing standards.

Copyright © 2013 State of Michigan

Because many of the pages in this document include embedded screen captures, page breaks have intentionally been added so that images and related textual information are kept contiguous. As a result, some pages may appear to be half filled with text.

This document includes images and text best viewed in color. Because of the state's current color printing restrictions, this document is best viewed on screen as a PDF or printed in color from your location.



Required Core Branding Elements

All application designs must incorporate these core elements for a common, consistent presentation layer:

Banner Header

Artwork supplied by eMichigan Web Development.

Sub Header

Directly under banner header and includes all utility links and required links.

Primary Application Display Area

Includes primary user interface and functionality. May utilize Body Only, Left Navigation Only or Left and Right navigation. Left and Right navigation are optional. In some instances Horizontal navigation may be allowed as long the Sub Header functionality is included.

Footer and Policy Links

Includes all required policy links, support sub header links and copyright information.

The diagram illustrates a web application layout with four key branding elements highlighted by callouts:

- Banner Header:** A green bar at the top containing the Michigan logo, the text "Agency or Application Name", "Parent Agency Name", and the "Michigan.gov" logo with the tagline "The Official State of Michigan Website".
- Sub Header:** A thin green bar below the banner header containing navigation links: "Michigan.gov Home", "Application Home", "Contact", and "Agency Home".
- Primary Application Display area:** The main content area, which in this example contains an "Example Form". The form includes a title, instructions, a section for "Organization Information" with required fields for "Organization", "Full Name", and "Email", and "Submit" and "Reset" buttons.
- Footer and Policy Links:** A white bar at the bottom containing a row of policy links: "Michigan.gov Home", "Application Home", "Contact", "Agency Home", "Accessibility Policy", "Privacy Policy", "Link Policy", and "Security Policy". Below the links is the copyright notice "Copyright © 2001-2005 State of Michigan".