SECU.01: MEDC Enterprise Security Control Policy

Michigan Economic Development Corporation
Information Technology

Topic Area: Policy for Michigan Economic Development Corporation Information Technology Information and Data Security.

Application: This policy is intended for Michigan Economic Development Corporation (MEDC) compliance and applies to all employees and Trusted Partners using the MEDC information systems and network and Information Technology (IT) resources.

MEDC Infrastructure Services Team is responsible for overseeing physical and IT security risk management, awareness, and training; assists MEDC business units with their security issues; and enforces oversight of MEDC security policies, standards, and procedures to maintain suitable levels of enterprise-wide security.

To secure the enterprise IT environment, MEDC Infrastructure Services Team has selected the cybersecurity framework published by the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), (Revision 4 – moderate controls) as the minimum security controls for MEDC information systems. Each System Security Plan will address NIST security standards and guidelines.

Purpose: MEDC Infrastructure Services is committed to securing MEDC 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 MEDC's facilities and systems. This policy establishes the MEDC strategic view of IT security in information systems that process, store, and transmit MEDC information. The MEDC Infrastructure Services Team must address security controls applicable to corresponding systems as addressed in this policy and corresponding standards and procedures.

Contact /Owner: Michigan Economic Development Corporation
Information Technology

Telephone: (517) 373-8600

Fax: (517) 241-8797

Summary: Security controls are implemented to protect MEDC information from unauthorized access, use, disclosure, modification, destruction, or denial and to ensure confidentiality, integrity, and availability of MEDC information. All MEDC employees, trusted partners, or entities authorized to access, store, or transmit MEDC information shall protect the

Issued Date:	Last Revision:	Last Reviewed:	Next Review Date:
November 17, 2016	July 2, 2018	July 2, 2018	July 2, 2019

confidentiality, integrity and availability of the information as set forth in this and all MEDC IT policies. Information is not limited to data in computer systems and is included wherever it resides in a business unit, 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 MEDC is considered MEDC 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 MEDC Information
- Authorization Prerequisites
- Acceptable Use of Information Technology
- Electronic Processing
- IT Network Infrastructure
- Database Security
- Sensitive Information

MEDC Infrastructure Services 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 MEDC *AUTH.01.001: 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 *MEDC AUTH.01.002: Technical Policy and Product Exception Standard.*

Policy:

GENERAL

The following MEDC standards are established in accordance with corresponding NIST baseline controls. Each MEDC business unit is bound to each standard. This policy establishes the standards and procedures to effectively implement corresponding MEDC Cyber Security baseline controls on the subject. All MEDC business units must adhere to a formal, documented policy that addresses purpose, roles, responsibilities, management commitment, coordination among MEDC entities, and demonstrates compliance with each of the following

standards that were developed and implemented by the MEDC Infrastructure Services Team. Each security policy, standard, and procedure must be reviewed and updated annually by the MEDC Infrastructure Services Team.

020 ACCESS CONTROL (AC-1)

MEDC IT Standard *SECU.01.020.01* establishes the Access Control standards in this MEDC 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 all MEDC 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)

MEDC IT standard *SECU.01.030.01* establishes the Security Awareness and Training standards in this MEDC 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 all MEDC personnel understand the responsibilities and training requirements necessary to effectively maintain organizational awareness, minimize insider threats, and prevent security related incidents.

040 AUDIT AND ACCOUNTABILITY (AU-1)

MEDC IT standard *SECU.01.040.01* establishes the Audit and Accountability standards in this MEDC policy.

These standards require MEDC Infrastructure Services 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 MEDC Infrastructure Services Team understand the responsibilities necessary to successfully manage audit information, assign audit roles and tasks, and prevent the compromise of MEDC information.

050 SECURITY ASSESSMENT AND AUTHORIZATION (CA-1)

MEDC IT standard *SECU.01.050.01* establishes the Security Assessment and Authorization standards in this MEDC policy.

These standards require MEDC Infrastructure Services to conduct impartial security and organizational assessments, establish external

system restrictions, and conduct penetration testing and other necessary vulnerability assessments. These standards ensure that the MEDC Infrastructure Services Team 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)

MEDC IT standard *SECU.01.060.01* establishes the Configuration Management standards in this MEDC policy.

These standards require MEDC Infrastructure Services Team to adequately manage the configuration of MEDC'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 MEDC Infrastructure Services Team 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)

MEDC IT standard *SECU.01.070.01* establishes the Contingency Planning standards in this MEDC policy.

These standards require the MEDC Infrastructure Services Team 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 MEDC Infrastructure Services Team understands 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 MEDC information.

080 IDENTIFICATION AND AUTHENTICATION (IA-1)

MEDC IT standard *SECU.01.080.01* establishes the Identification and Authentication standards in this MEDC policy.

These standards require MEDC Infrastructure Services Team 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 MEDC Infrastructure Services Team and third parties understand the responsibilities necessary in order to regulate non-privileged access of MEDC accounts, minimize authentication attacks, and prevent unauthorized devices and connections with MEDC networks.

090 INCIDENT RESPONSE (IR-1)

MEDC IT standard *SECU.01.090.01* establishes the Incident Response standards in this MEDC policy.

These standards require the MEDC Infrastructure Services Team to apply incident response capabilities, including automated response and reporting processes, establish a test process for those incident response capabilities, and coordinate with existing MEDC contingency plans. These standards ensure that MEDC Infrastructure Services Team and all other associated personnel understand the responsibilities necessary to ensure the MEDC'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)

MEDC IT standard *SECU.01.100.01* establishes the Maintenance standards in this MEDC policy.

These standards require the MEDC Infrastructure Services Team to employ adequate and approved information maintenance tools, inspect all maintenance tools entering MEDC facilities, including supporting media, and apply priority or time-sensitive maintenance procedures. These standards ensure that the MEDC Infrastructure Services Team understands the responsibilities necessary to effectively diagnose and repair MEDC information systems, ensure maintenance tools and supporting media are not modified beyond the MEDC'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)

MEDC IT standard *SECU.01.110.01* establishes the Media Protection standards in this MEDC policy.

These standards require the MEDC Infrastructure Services Team 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 MEDC Infrastructure Services Team understand the responsibilities necessary to ensure all MEDC 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)

MEDC IT standard *SECU.01.120.01* establishes the Physical and Environmental Protection standards in this MEDC policy.

These standards require definition of both physical facility and information system management processes. The MEDC Infrastructure Services Team 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 MEDC Infrastructure Services Team understand the responsibilities necessary to prevent unauthorized communication or transmission access, maintain access records, minimize the compromise of sensitive output information, and protect MEDC equipment, facilities and environments, including emergency power procedures and relocation contingencies.

130 SECURITY PLANNING (PL-1)

MEDC IT standard *SECU.01.130.01* establishes the Security Planning standards in this MEDC policy.

These standards require the MEDC Infrastructure Services Team 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 MEDC Infrastructure Services Team understand the responsibilities necessary to prevent security activity conflicts within and throughout the MEDC, prevent negative impact and restraints on other organizations, minimize unauthorized access to MEDC information available on public information sites, and ensure a proper security architecture is in place and is continuously assessed.

140 PERSONNEL SECURITY (PS-1)

MEDC IT standard *SECU.01.140.01* establishes the Personnel Security standards in this MEDC policy.

These standards require that the organization employs automated mechanisms to control both MEDC 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 MEDC understands 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)

MEDC IT standard *SECU.01.150.01* establishes the Risk Assessment standards in this MEDC 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 the MEDC Infrastructure Services Team understands the responsibilities necessary to readily identify and respond to system vulnerabilities.

160 SYSTEM AND SERVICES ACQUISITION (SA-1)

MEDC IT standard SECU.01.160.01 establishes the System and Services Acquisition standards in this MEDC 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 the MEDC Infrastructure Services Team understands the responsibilities necessary to ensure that MEDC 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)

MEDC IT standard *SECU.01.170.01* establishes the System and Communications Protection standards in this MEDC policy.

These standards require that the MEDC Infrastructure Services Team 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 MEDC understands 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)

MEDC IT standard *SECU.01.180.01* establishes the System and Information Integrity standards in this MEDC policy.

These standards require that the MEDC Information Technology Team 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 MEDC understands the responsibilities necessary to effectively determine changing states within the MEDC's information systems, obtain accurate event-based system information, and determine suitable corrective actions for security-relevant events.

ROLES AND RESPONSIBILITIES

Infrastructure Services, Director:

As a Data Owner, the Infrastructure Services, Director shall ensure:

- Data management is compliant with federal and state laws and regulations, and MEDC policies.
- Information security controls are implemented to protect the MEDC information and that these controls are sufficient to ensure the confidentiality, integrity, and availability of MEDC 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.
- MEDC business unit information is identified and classified based on sensitivity, criticality and risk in compliance to federal and state laws and regulations, and includes a review at least once a year, or when the environment changes, of the on-going requirement to continue protection.
- A system is established to identify baseline security controls to protect MEDC 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.
- MEDC business unit information is safeguarded with the proper controls in accordance with its classification label.
- Data, which is shared or transferred between business units, is protected by the receiving business unit with at least the same level of security used by the sending business unit. The receiving business unit 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 business unit must obtain permission from the Business Owner.
- Controls are established to provide MEDC oversight of trusted partners who handle MEDC information on behalf of the MEDC.
- MEDC business unit information is disposed of and sanitized in compliance with MEDC 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. A system is established to review technical controls and recommendations identified by the MEDC IT Data Center Team.

- Internal business unit security policies and procedures are implemented, maintained and enforced that compliment and comply with this policy.
- All MEDC employees and trusted partners handle information for which they are responsible in compliance with this policy and all MEDC IT policies.
- MEDC employees and trusted partners are trained to ensure they are aware of their role in protecting MEDC information and data as set forth in this policy.
- Employees are advised of the necessity of complying with MEDC policies and laws pertaining to the protection of MEDC information, because non-compliance may leave the state, and/or MEDC, liable and employees vulnerable to prosecution and civil suit, as well as disciplinary action.

MEDC CIO: As a Data Custodian, the Chief Information Officer (CIO) shall ensure:

- Business units are advised as to the best operational and technical controls necessary to protect their data in accordance with its classification label.
- Business unit-prescribed security controls and safeguards are implemented and monitored for compliance.

MEDC IT: MEDC IT is responsible for establishing an enterprise information security program. The program shall include 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.

MEDC IT shall:

- Align the enterprise information security program, its activities, and staff with the requirements of the policies defined in the Security Program.
- Establish a governance body to direct the development of MEDC specific information security plans, policies, standards, and other authoritative documents.
- Oversee the creation, maintenance, and enforcement of established enterprise information security policies, standards, procedures, and guidelines.
- Ensure that MEDC security policies and procedures are fully documented and MEDC business units are aware of, have agreed to

comply with, and understand the consequences of failure to comply with policies and procedures.

- Identify and integrate or align enterprise information security goals and objectives to the MEDC business units strategic and tactical plans.
- Develop and track information security and privacy risk key performance indicators.

Terms And Definitions:

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 Unit: A unit of organization within the MEDC.

Confidentiality: Protecting information from unauthorized disclosure or interception 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: MEDC information. No distinction between the words data and information are made for purposes of this policy.

Data Owner: An individual or business Unit who is ultimately responsible for ensuring the protection, use and accuracy of data.

Enterprise: MEDC wide.

Information Technology (IT) Resources: Includes, but is not limited to, devices, networks, data, software, hardware, email, system accounts, and facilities provided to conduct official MEDC business.

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. Integrity considers all possible causes of modification, including software and hardware failure, environmental events, and human intervention.

Technical Policies: 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.

Authority:

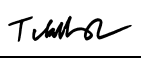
- Executive Order No. 1999-1, formation of the MEDC.
- Executive Order No. 1999-1 and assigning IT staff to the MEDC for the purpose of the administration of MEDC technology usage.
- The *AUTH.01: MEDC Information Technology* policy is the mechanism for establishing an enterprise approach to IT management and serves as the overarching umbrella policy for MEDC information and assets

Enforcement: Any MEDC employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or criminal prosecution where the act constitutes a violation of law.

Any MEDC Trusted Partner found to have violated this policy may be subject to action, up to and including criminal prosecution where the act constitutes a violation of law. A breach of contract and fiduciary liability may also apply.

Exceptions: Exceptions to any IT PSP can be requested through the IT Helpdesk. All exception requests will go through the normal PSP change procedure. The Requestor will be asked to explain their request at a meeting of the Cross Functional Review Team meeting.

Effective Date: November 17, 2016

Signature and Title of Approver:	**Date:**
Tilak Mohan, Chief Information Officer 	November 17, 2016

Author:	Approver:	Approval Date:	Description of Change(s):
Kim Fedewa	Tilak Mohan	November 17, 2016	Original copy approval.
Kim Fedewa	Tilak Mohan	July 2, 2018	20 grammatical errors, added all Trusted Partner references.