MICHIGAN ECONOMIC DEVELOPMENT CORPORATION	**MICHIGAN ECONOMIC DEVELOPMENT CORPORATION** Information Technology	**Standard:** **INFRA.01.006**
Topic Area:	**Elevated Access Rights Standard**	
Distribution:	**All Michigan Economic Development Corporation Staff**	

Purpose: To define a standard for requesting elevated rights to any Michigan Economic Development Corporation (MEDC) system for authorized employees, contractors, and vendors who require elevated access to perform the responsibilities of their job for a limited period of time with a justified purpose.

Contact/Owner: Michigan Economic Development Corporation
Information Technology

Scope: This scope governs the administration of all systems in the MEDC Information Technology (IT) managed environment.

Standard: Elevated Rights are permissions above and beyond a normal user's permissions.

Only an MEDC Data Center authorized member or the Infrastructure Services, Director can approve or decline requests for elevated rights to MEDC systems.

All elevated rights are considered temporary in that the maximum time the elevated rights will be issued is for one year.

MEDC Network Administrators will need to request elevated rights. MEDC Network Administrators elevated rights will auto renew at the end of each year. Their elevated rights will be revoked upon a change of roles within the MEDC where the elevated rights are no longer needed or their departure from the MEDC.

The MEDC IT staff will maintain a list of all elevated rights requested, approved or denied, and active or closed. This list will include the user name, date granted or denied, ending date of elevated rights, the status of the request, the specific rights given. This list will be updated whenever elevated rights, for a user or non-user account, are granted, modified, terminated, or denied.

Requirements for requesting elevated rights on any or all MEDC IT systems are as follows:

- **Requirements for Requesting Elevated Rights**: MEDC IT network administrators require detailed information about the authorized personnel or vendor requesting rights to the MEDC servers.

1. A helpdesk ticket is created containing the following:
    a. The name of the person requesting elevated rights.
    b. The start date and time and the end date and time of the request.
    c. The business reason for the elevated rights.
    d. Detailed information about the work being performed.
    e. Detailed info about the desired outcomes.
2. Elevated Rights for non-MEDC Network Administrators will be temporary and finite.
    a. All attempts must have been made to accomplish the desired outcomes without the elevated rights prior to approval.
    b. Following the guidelines of the MEDC IT, elevated rights are allowed for the time frame specified in the helpdesk ticket or for one year, whichever is the smaller amount of time.
3. Elevated rights can be denied for any reason including but not limited to:
    a. Request is deemed out of the realm of the roles and responsibilities of the requester.
    b. Proper authorization and approval is not provided.
    c. Helpdesk ticket does not have adequate information such as who is performing the job, what is being done – in detail, and why it is being done.
    d. Length of time requested is too long as deemed by the Infrastructure Services, Director and the Data Center Authorized personnel.
4. Testing updates, system changes, and maintenance must be performed in a test environment prior to implementation in the production environment, if possible.
5. User sessions will have the following limits unless a server falls under a more restrictive regulatory requirement.
    a. A disconnected session will auto end after 12 hours.
    b. An active session limit of 12 hours, then auto end session.
    c. An idle session limit of 12 hours, then auto end session.
6. Elevated rights that have expired, can only be reinstated by going through a new Requesting Elevated Rights process.

Elevated Rights on Windows Servers: All servers supported by MEDC IT within the MEDC's environment will adhere to the MEDC approved elements of the *National Institute of Standards and Technology (NIST) SP 800-123, Guide to General Server Security* and industry best practices when elevated rights are requested.

1. To enforce separation of duties between server administrators and application administrators, Domain Groups shall be created for all windows servers within the MEDC domains for the purpose of managing elevated rights.

   Example: Admins =(hostname) Admin

   Example: Power User =(hostname) PU

   a. The Domain Groups created for temporary elevated rights will use the least privilege principle. This group shall remain empty unless elevated rights have been approved and assigned.

2. **Exception:**

   a. If elevated rights are needed that do not follow the accepted process or "best practices", *AUTH.01.002: Policy and Product Exception Process Standard* must be followed.

   b. If the ticketing system is unavailable, the requestor may contact the Helpdesk or Data Center Support Team directly to effect the change to elevated rights. All documentation and ticketing tasks described above in Step 1 of Requirements for Requesting Elevated Rights will be required when the ticketing system is available.

Administrative Auditing: A monthly audit of elevated rights will be performed by the Client Technology Services team to validate that assigned elevated rights are required, granting or removal of elevated rights was properly documented, that granted elevated rights match what was documented, and that expired elevated rights were removed.

Glossary:

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.

Data/Information: MEDC business unit information. No distinctions between the words data and information are made for the purposes of this procedure.

Data Custodian: An individual or organization that has responsibility delegated by a data owner for maintenance and technical management of data and systems.

Data Owner: An individual or organization who is ultimately responsible for ensuring the protection and use of data.

Authoritative Policies:	INFRA.01
Associated Procedures:	INFRA.01.006.01

Signature and Title of Approver:	**Date:**
Tilak Mohan, Chief Information Officer Digitally signed by Tilak Mohan DN: cn=Tilak Mohan, o=Michigan Economic Development Corporation, ou=Information Services, email=mohant1@michigan.org, c=US Date: 2018.05.04 19:03:48 -04'00'	April 30, 2018

Author:	**Approver:**	**Approval Date:**	**Description of Change(s):**
Kim Fedewa	Tilak Mohan	November 17, 2016	Original copy approval.
Kim Fedewa	Tilak Mohan	April 14, 2017	Renamed Standard, Added verbiage about Net Admins, Added verbiage about maintaining list.
Kim Fedewa	Tilak Mohan	April 30, 2018	In item 5, changed fails to falls. In Elevated Rights on Windows Servers, changed verbiage to read “been approved and assigned.”

Issued Date:	**Last Revision:**	**Last Reviewed:**	**Next Review Date:**
November 17, 2016	April 30, 2018	April 30, 2018	April 30, 2019