Section Name: Information Security Effective Date**:** September 3, 2019
Section Number: 800
Policy Number: 805

Subject: Access Management

Overview: Protecting access to Information Technology (IT) Systems and applications is critical to maintain the integrity of Monroe County's technological and data and prevent unauthorized access to such resources. Access to Monroe County systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

Purpose: The objective of this policy is to ensure the County has adequate controls to restrict access to systems and data by providing appropriate access authorization.

Scope: This Policy applies to all employees, elected officials, judges, contracted staff, vendors, or any other individual or organization/agency that requests or requires access to the Monroe County network.

Monroe County IT Department or their designee will provide access privileges to network systems, applications, computers and mobiles devices based on the following principles:

A. Need to know – individuals or organizations will be granted access to systems that are necessary to fulfill their roles and responsibilities.
B. Least Privilege – individuals or organizations will be provided with the minimum access privileges necessary to fulfill their roles and responsibilities.
C. Documentation – all access must be documented and have a documented purpose.

Statement of Policy:

A. Requests for users' or organizations' accounts and access privileges must be conveyed in writing (email, request ticket, etc.). Users may not request privileges for themselves; the request must be approved by their supervisor or other person with authority. Organizations (vendors, State of Michigan, other local governments, etc.) must contact the IT Department directly.

B. Application and service accounts must be used only by application components requiring authentication; access to application and system passwords must be restricted to authorized IT administrators or application vendors.

C. Requests for special accounts and privileges (such as vendor accounts, shared / generic accounts, test accounts, remote access, etc.) must be documented and approved by the system owner or IT Director.

D. Account expiration:

    1. When temporary access is required, such access will be removed immediately after the user has completed the task for which access was granted.

2. User accounts assigned to contractors will be set to expire according to the contract expiration date.
3. Local computer and network accounts will be disabled after ninety (90) days of inactivity.
4. Special accounts and privileges will be disabled after fourteen (14) days of inactivity

E. Access rights will be immediately disabled or removed upon notification that the user has been terminated or ceases to have a legitimate reason to access Monroe County systems.

F. Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples include:

1. An active account assigned to external contractors, vendors or employees that no longer work for the Monroe County.
2. An active account with access rights for which the user's role and responsibilities do not require access.
3. System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
4. Unknown active accounts.

G. Shared user accounts:

1. Where possible, the use of specific network domain "security groups" should be used to share common access permissions across many users, instead of shared accounts.
2. Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as "guest" and "functional" accounts.
3. When shared accounts are required:
    a. Passwords will be stored and handled in accordance with the Password Policy.
    b. The use of shared accounts will be monitored where possible, including the recording of time of access, the reason for accessing the shared user account, and the individual access for this account.

H. Vendor or Default Accounts:

1. Where possible, all default user accounts will be disabled or their passwords changed. These accounts include "guest", "temp", "admin", "Administrator", and any other commonly known or used default accounts, as well as related default passwords used by vendors on "commercial off the shelf" systems and applications.

I. Test Accounts:

1. Test accounts can only be created if they are justified by the relevant business area of a project team and approved by the application owner, through a formal written request to the IT Director or the IT Help Desk.
2. Test accounts must have an expiration date. Test accounts will be monitored and reviewed every six (6) months.
3. Test accounts will be disabled and/or deleted when no longer necessary.

J. Contractors and Vendors

1. Contractor and vendor representatives will be required to sign a Non-Disclosure Agreement (NDA) [and acknowledge relevant access policies] prior to obtaining approval to access Monroe County systems and applications.
2. Prior to granting access rights to a contractor / vendor, the IT Director or Help Desk must verify the requirements.
3. The name of the contractor / vendor representative must be communicated to the IT Department at least two (2) business days before the person needs access.
4. The County IT Department will maintain a list of external contractors / vendors having access to County systems.
5. The need to terminate the access privileges of the contractor / vendor must be communicated to the IT Department at least one (1) business day before the contractor / vendor representative's access needs to end.

Policy Compliance:

A. Responsibility-All Elected Officials/Judges/Department Heads, or their designee(s), are responsible for implementing the policies and procedures and ensuring staff compliance in their respective areas.

B. Compliance measurement - The IT Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits.

C. Exceptions – Any exceptions to the policy must be approved by the IT Department and Department Head or Elected Official for whom the employee works.

D. Non-Compliance – An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract.

Definitions: NA

Administrative Procedures: None

Legislative History of Authority for Creation or Revision:

Adopted pursuant to action of the Monroe County Board of Commissioners, dated September 3, 2019.