LAST UPDATE DATE	04-03-2025
OWNER	JEFF LILLIBRIDGE
STATUS	APPROVED

ACCESS MANAGEMENT POLICY

Approval History

Version	Approved By	Approved On
1.0	Not Present	04-03-2025

Purpose

The purpose of the Access Management Policy is to define the level of access each user has to company-owned or managed information systems and the data in City of Madeira Beach's systems.

Scope

The Access Management Policy applies to the following:

- All full-time, part-time, or temporary employees
- All third-party vendors, contractors, and visitors who temporarily access the Company's equipment
- All information systems owned and/or managed directly by City of Madeira Beach
- All data repositories belonging to City of Madeira Beach

Background

The Access Management Policy defines the rules and processes put in place to help prevent unauthorized access to information systems and resources owned by City of Madeira Beach. Unauthorized access may be malicious actors outside of the organization trying to come in, malicious insiders trying to gain access to resources they should not have access to, or unintentional access by employees who inadvertently access something that they otherwise should not have access to without any malicious intent. In any case, failure to properly manage user access may result in a wide range of issues from unintentional data modification to data theft or even regulatory fines and legal actions against the organization. To combat this, effective access management policies and procedures must be implemented to ensure that only approved individuals gain access to only what is necessary to carry out their normal duties.

Policy

Types of Accounts

The following accounts should be employed (at a minimum) across all information technology systems where technically feasible:

- Administrator/privileged accounts (with Superuser access) - Accounts that are provisioned with elevated privileges for the purposes of administering the system, managing the system, or otherwise performing actions within the system that require elevated privileges.
- User accounts - General purpose accounts to be used for performing regular actions within the system.
- System accounts - Accounts that have been included within the system as a necessity to its functionality. These will likely be pre-installed by the system's manufacturer.

General User Access Management

- All employees, contractors, and third-party users are assigned a unique identifier (i.e., username) when first provisioning system access. These unique identifiers may not be reused between multiple users such as if an individual is onboarded with the same name as an individual who was previously employed by the Company. The only exception to this is if a prior employee is rehired at a later time.
- Where technically feasible, systems should enforce the use of multifactor authentication (MFA). Alternatively, this may be accomplished through the use of single sign-on (SSO).
- Each information system must enforce the password and login restrictions based on the Company's password policy.
- Each information system should define, document, and implement its unique access management covering all aspects of the user lifecycle from onboarding to offboarding. This should be documented in the system security plan (SSP).
- Where technically feasible, user access permissions should be provisioned through the use of RBAC. To do this, users must be grouped by roles based on factors such as the following:
    - Business unit they belong to (e.g., Information Technology, Human Resources, Executive Leadership, etc.)
    - Specific role they perform (e.g., system administrator, recruiter, manager, etc.)
    - Employment status (e.g., full-time employee, part-time employee, contractor, etc.)

New User Onboarding

- Managers of new employees must request the provisioning of user accounts to all necessary systems and data prior to the new employee's first day.
    - Requests for new user accounts must be submitted in writing via the appropriate channels.
    - Once approved or denied, all requests must be retained based on the Company's Data Retention Policy.
    - For regular user accounts, approval must be obtained from the appropriate system owner or delegate.

    - For administrator/privileged accounts, approval must be obtained from the employee's manager as well as the system owner or delegate. Where the system owner is the same as the employee's manager, additional approval must be obtained by the Department Head or delegate.
    - For administrator/privileged accounts, justification must be included in the original request supporting why the user requires such access to support their normal job duties.
    - All access requests must be time-bound, requiring regular review of access permissions.

User Offboarding

- A user's manager must request system access be revoked by the close of business on an employee's last day of employment with the Company in all cases of voluntary termination.
- In all cases of involuntary termination, an employee's manager must request the user's access permissions be revoked in line with the timing of the employee's notification of termination.
- For voluntary and involuntary terminations, a user's account need only be disabled according to the timing noted above.
- Confirmation of the revocation of a user's access permissions should be provided to Human Resources in all cases to be included as a part of each employee's records. This confirmation must also be provided to the user's manager.

Elevated Access Management

- Elevated access requests must be submitted by a user's manager and must include, at a minimum, the following:
    - Name of user that access is being requested for
    - Name of manager
    - User's department
    - User's job title
    - Date of request
    - Date of expiration of access approval (not to exceed one year)
    - Reason for request
    - Detailed justification for granting access
    - Dated approval by user's manager
    - Dated approval by system owner or Department Head if the system owner is the same as the user's manager
- Elevated access should follow the principle of least privilege and only be requested for systems which the user must have this access.
- Elevated access must be reviewed at least every six months to ensure that the users with elevated access are still in the roles requiring elevated permissions.

Access Management for Third Parties/Contractors

- All access requests for third parties and contractors should follow the same process as mentioned in the sections above.

- All third parties and contractors must be granted access to user groups set up specifically for such users (i.e., not given access to general user groups or administrator groups).
- Access for third parties and contractors must be enabled for the approved period during which their partnership agreement or contract is valid. Any additional time required will need to be requested through a separate access request.
- Remote access to third-party contractors must be provided only after a formal request and only where absolutely necessary. This access must be configured to be valid for the minimum time possible and must require submission of a new request should additional time be required.

Password and Other Authentication Mechanisms

- Where technically feasible, all information systems must enforce the use of MFA or SSO for logging in.
- Please refer to the Password Protection Policy for additional details.

Audit and Logging

- All user access to information systems must be logged.
- At a minimum, logs must contain the following:
    - Unique user ID
    - Date and time of login based on internal system clock
    - Result of the login attempt (i.e., access granted, login failed, etc.)
- All logs must be stored for at least 60 days.
- All logs must be ingested into a central repository for storage, analysis, and alerting or be configured to automatically alert for malicious access attempts (e.g., multiple failed login attempts in a short time period) or be reviewed manually on a weekly, bi-weekly, or monthly basis depending on system criticality.

Enforcement

The Access Management Policy is enforced by all System Administrators and Department Heads. Any exceptions to this policy must be reviewed and approved by the Information Security Team. Any breach of this policy may result in disciplinary actions up to and including termination of employment.