| | |
|---|---|
| LAST UPDATE DATE | 04-24-2025 |
| OWNER | JEFF LILLIBRIDGE |
| STATUS | APPROVED |

# REMOTE ACCESS POLICY

Approval History

| Version | Approved By | Approved On |
|---|---|---|
| 1.0 | Not Present | 04-24-2025 |

# Purpose

The purpose of the Remote Access Policy is to outline the rules and procedures for remote hosts to connect to City of Madeira Beach's corporate network.

# Scope

Remote Access Policy applies to the following:

- All Remote Work (aka, Teleworking) Employees and Contractors of City of Madeira Beach.
- Organizations network
- Mobile computing devices
- Remote clients such as laptops, computers

# Background

The objective is to secure remote work environments and prevent loss, damage, theft, or compromise of assets and interruption to the Company's operations. Accidental or intentional exposure of confidential data within a company's network by not following proper procedure to connect to it is a huge risk faced by information security teams today. Hackers and other bad actors frequently use vulnerabilities on personal devices and home networks to conduct massive hack attacks on the company's network.

# Policy

This policy outlines all measures in place at City of Madeira Beach to minimize the exposure which results from such incidents.

**The organization**

- Documents allowed methods of remote access to the system;
- Establishes usage restrictions and implementation guidance for each allowed remote access method;
- Monitors for unauthorized remote access to the system;

- Authorizes remote access to the system before connection; and
- Enforces requirements for remote connections to the system.

**Company IT security personnel are responsible for:**

- Documenting allowed methods of remote access to the system;
- Establishing usage restrictions and implementation guidance for each allowed remote access method;
- Monitoring for unauthorized remote access to systems;
- Authorizing remote access to systems prior to connection;
- Enforcing requirements for remote connections to systems;
- Using cryptography to protect the confidentiality and integrity of remote access sessions;
- Automatically disconnecting remote access sessions after a period of inactivity; and
- Immediately deactivating vendor and business partner remote access when it is no longer needed.
- The Company authorizes remote users to connect to City of Madeira Beach information assets only if the following criteria for the remote system are met:
- Software patch status is current; and
- Anti-malware software is enabled and current.

Security shall be applied to off-site assets considering the different risks of working outside the organization's premises. City of Madeira Beach asset custodians and data owners are required to maintain strict control over the internal or external distribution of media, including the following:

- Classifying media per Data Classification & Handling Guidelines so the sensitivity of the data can be determined;
- Sending sensitive media by secured courier or other delivery methods that can be accurately tracked; and
- Ensure prior management approval for any media moved from a secured area (including when media is distributed to individuals).

**Security requirements for remote hosts**

- Remote hosts are configured as per the Configuration Management policy
- Remote hosts have all the latest security patches and antivirus installed
- Remote hosts have the latest and most updated endpoint protection software (e.g. malware scanner) installed
- Information stored on mobile computing equipment must be encrypted using hard drive full disk encryption.

**VPN Access**

- Access to an organization's network is only allowed via VPN which is maintained by the IT team
- VPN access is only granted by the IT team and requires user-level authentication and credentials to connect to the organization's network

**Security Requirements for Teleworkers and their environment**

- Employees must be specifically authorized for telework in writing by their hiring manager.
- Only the device's assigned owner is permitted to use remote nodes and mobile computing equipment. Unauthorized users (such as others living or working at the location where telework is performed) are not permitted to use such devices.
- Users performing telework are responsible for the appropriate configuration of the local network used for connecting to the Internet at their telework location.
- Users performing telework must protect the Company's intellectual property rights, either for software or other materials that are present on remote nodes and mobile computing equipment.

# Enforcement

The information security team and IT Team staff are accountable for enforcing remote access policy requirements. Failure to adhere to this policy might lead to disciplinary actions.