LAST UPDATE DATE	04-18-2025
OWNER	JEFF LILLIBRIDGE
STATUS	APPROVED

ANTIVIRUS POLICY

Approval History

Version	Approved By	Approved On
1.0	Not Present	04-03-2025
2.0	Not Present	04-18-2025

Purpose

The Antivirus Policy aims to protect City of Madeira Beach systems from malware threats. It will be reviewed and updated annually or as required by changes in the threat landscape or regulatory requirements.

Scope

The Antivirus Policy applies to all hardware and software owned, managed, and/or utilized City of Madeira Beach, where technically feasible.

Background

New viruses are discovered almost every day. Therefore, it is necessary for organizations to adopt a standard approach to deploy anti-virus applications throughout their environment. The anti-virus solution or software should guard against malicious software or scripts by blocking or quarantining the malicious software that is identified, and alerting administrators that such action has taken place.

Policy

Antivirus Software Deployment

- All company-owned devices, including workstations, laptops, servers, and mobile devices, must have approved antivirus software installed and actively running.
- The antivirus software shall be centrally managed and monitored by the Managed Services Provider (MSP).

Updates and Scans

- Antivirus software must be configured to automatically update virus definitions at least daily.
- Full system scans must be scheduled to run at least weekly on all devices.
- Real-time scanning must be enabled on all devices to provide continuous protection.

User Responsibilities

- Users are prohibited from disabling or interfering with antivirus software operations.
- Users must report any suspicious files or potential infections to the MSP for further investigation.

Incident Response

- In the event of a detected threat, the antivirus software must automatically quarantine the suspicious file.
- The MSP shall investigate the potential threat to determine if there's been any impact to the organization.
- If necessary, activate the incident response plan and follow all required steps to respond to and neutralize the threat to the organization.

Removable Media

- All removable media (e.g., USB drives, external hard drives) must be scanned by the antivirus software before accessing any files.

Logging and Monitoring

- Antivirus logs must be collected and retained for a minimum of 12 months.
- The MSP shall review antivirus logs regularly for any patterns or indicators of compromise.

Compliance and Auditing

- Annual audits of antivirus deployment, configuration, and effectiveness must be conducted.
- Any devices found to be non-compliant with this policy must be immediately remediated or disconnected from the network.

Enforcement

This policy shall be enforced at all times. Any deviations from the policy require a documented written request and formal approval by Senior Management. Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.