City of Waukesha
Malware Defense Policy

I. Purpose. Malware defense includes the configuration, maintenance, detection, reporting, and remediation of anti-malware software and the malware it identifies. The Malware Defense Policy provides the processes and procedures to accomplish those tasks. This policy applies to all departments and all assets connected to the enterprise network.

II. Definitions.

A. Device means any City-owned or City-issued desktop computer, laptop computer, notebook computer, tablet, mobile phone, or other communications equipment.

B. User means any individual who operates a Device, regardless of whether that individual is a City employee or not.

C. Malware means any malicious software intended to steal data, and disrupt, damage or destroy computers and computer systems. Common malware includes viruses, worms, Trojans, adware, spyware, and ransomware.

D. Anti-malware means the software approved by the IT Department for installation on Devices to detect, block, and remove malicious software and other security threats.

III. IT Responsibility. The IT business unit is primarily responsible for malware defense. Specifically, administrators are responsible for configuring the correct devices to generate, store, and transmit logs. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them. All enterprise assets are required to comply with the malware defense policy and procedures.

A. Configuration. IT must install anti-malware software on all enterprise assets where appropriate

B. Update.

1. Anti-malware software must be configured to automatically update.

2. IT must ensure that anti-malware signatures are kept up-to-date as they become available via an automatic update process.

3. Operating systems must be configured to automatically update, unless an alternative approved patching process is used.

C. Detection. IT must ensure that anti-malware software is properly functioning on all enterprise assets.

D. Reporting.

1. All confirmed high severity alerts must be reported to the User.

2. The presence of unauthorized software must be properly investigated.

E. Remediation.

1. Identified malware must be removed from enterprise assets.

2. Unauthorized software must be removed from use on enterprise assets or receive a documented exception.

IV. User Responsibility. The following rules apply to all Users and must be followed at all times.

A. Configuration.

1. Users must not disable anti-malware software on their enterprise assets.

2. Users must not modify the update frequency

B. Update.

1. Users are responsible for connecting their devices to the enterprise network, regularly applying malware signature updates, and restarting their devices as appropriate. Anti-malware must always be configured to run periodic scans automatically, and this configuration cannot be altered by Users.

2. Whenever Anti-malware prompts a User to update or to run a scan, the User shall respond to the prompt by allowing the update or run the scan. Users may not respond to prompts by refusing the action suggested by the Anti-malware.

C. Detection.

1. All removable media (for example, USB thumb drives) must be scanned using Antivirus before being used.

2. All files downloaded from the internet or attached to emails must be scanned using Antivirus before being used.

D. Reporting.

1. All confirmed high severity alerts must be reported to the IT Department.

2. If removable media are inserted and Antivirus does not immediately commence an automatic scan of the media, the media must be removed, and the IT Department notified.

3. If files are downloaded and Antivirus does not immediately commence an automatic scan of the media, the files must not be opened, and the IT Department must be notified.

E. Remediation.

1. Emails and email attachments coming from suspicious or unknown sources must not be opened. All such emails and attachments should be reported using the "Phishing Alert" button in Outlook. No such emails and attachments may be forwarded to any other User.

2. All directions given by the IT Department regarding Devices and Anti-malware must be followed at all times.

V. Penalties for Violations. Violations of these rules will subject the User to discipline, up to and including termination, as provided in Human Resources Policy G-3.

Passed by the Information Technology Board on the 3rd day of January 2024.
Approved by the Common Council on the 16th day of January 2024.

Shawn N. Reilly, Mayor

, Clerk-Treasurer