

**City of Waukesha**

201 Delafield St. Waukesha, WI 53188

Tel: 262.542.3700

waukesha-wi.gov

<b>Committee:</b> Information Technology Board	<b>Date:</b>
<b>Common Council Item Number:</b> #25-00540	<b>Date:</b> 2025-04-02
<b>Submitted By:</b> Chris Pofahl	<b>City Administrator Approval:</b> Chris Pofahl
<b>Finance Department Review:</b> Joseph P. Ciarro	<b>City Attorney's Office Review:</b> Brian Running
<b>Subject:</b> Malware Defense Policy	

**Details:**

Malware is one of the most common threats facing an enterprise. Malware can be used to capture credentials, steal data, identify other targets within the network, and encrypt or destroy data. Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, removable media, and more. Often, malware relies on insecure end-user behavior, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives into systems. Modern malware is designed to avoid, deceive, and disable defenses. Therefore, malware defenses must be able to operate in a dynamic environment through automation, timely and rapid updating, and integration with other processes like vulnerability management and incident response. Defenses must be deployed at all possible entry points and enterprise assets to detect, prevent spread, or control the execution of malicious software or code.

The CIS Critical Security Controls recommends a policy to govern defensive mitigations to prevent malware from compromising enterprise assets. There has been an Antivirus Policy in place since May of 2018. This Malware Defense Policy will replace the existing Antivirus Policy.

**Options & Alternatives:**

N/A

**Financial Remarks:**

N/A

**Executive Recommendation:**

Approve the Malware Defense Policy