


<b>Policy Title:</b>	<b>Virus and Malware Prevention and Detection Policy</b>		
	<b>OFFICE OF CHIEF INFORMATION OFFICER</b>	<b>Category</b>	Information Technology Services (ITS)
		<b>Administrative Policy #</b>	
		<b>Revision #</b>	
		<b>Review Frequency</b>	As Needed – no less frequently than triennially
<b>Administrative Division</b>	Information Technology Services (ITS)	<b>Reviewed By</b>	Chief Information Officer
<b>BOWC Approval</b>		<b>Last Reviewed/Update Date</b>	
<b>Implementation Date</b>			

## 1. OBJECTIVES

- 1.1. To ensure processes and systems are in place for the prevention and detection of potential security incidents caused by viruses and malware.

## 2. PURPOSE

- 2.1. To establish responsibilities and provide guidelines for users in the protection of DWSD's resources against intrusion by viruses and other malware, thus helping to ensure the security of the data and IT resources within DWSD.

## 3. DEFINITIONS

“Malware” refers to software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

“Virus” refers to malicious software that spreads by attaching itself to files or creating files that may be executed in some way for an unauthorized purpose.

## 4. SCOPE

- 4.1. This Virus and Malware Prevention and Detection Policy applies to all computer equipment operated by the organization or functioning on the organizational network. All third parties operating computer equipment on the organizational network must have an acceptable anti-virus solution which is kept current and active.

## 5. RESPONSIBILITIES

### 5.1. Chief Information Officer (CIO)

- 5.1.1. The Chief Information Officer (CIO), or delegate, is responsible for publishing this policy and updating this policy as necessary.
- 5.1.2. The CIO, or delegate, is responsible for interpreting and enforcing this policy.

## **5.2. Department of Innovation and Technology (“City” or “DoIT”)**

- 5.2.1. The City of Detroit’s Department of Innovation and Technology (“City” or “DoIT”) is responsible for providing the enterprise networking, applications and security services.
- 5.2.2. The City is responsible for ensuring that all servers have anti-virus and malware software installed and active. This includes real-time “on-access” scanning and weekly scan for malicious code.
- 5.2.3. In addition to having the standard anti-virus program, the email server or proxy server will include a second product which will be used to scan all email for viruses and/or malware. This scanner will scan all emails upon entry to the server and scan all emails before leaving the server. In addition, the scanner may scan all stored email periodically for viruses or malware.
- 5.2.4. The City is responsible for monitoring the effectiveness of the anti-virus protection systems and shall keep records detailing virus incidents on a monthly basis.
- 5.2.5. Refer to the City’s Virus and Malware, or related policy for more information.

## **5.3. Third Parties**

- 5.3.1. All third parties operating computer equipment on the organizational network must have an acceptable anti-virus solution which is kept current and active.

# **6. POLICY**

## **6.1. Prevention and Detection by DWSD Employees**

- 6.1.1. Users should know the type of file being opening and should have their computer system configured to show all file types and extensions.
- 6.1.2. Users should not open email attachments that are suspicious and only open attachments when they know it was really sent by the person who is claimed.
- 6.1.3. Users should be aware that a sender name may be spoofed or misrepresented in the email.
- 6.1.4. Users should report suspicious e-mails through the Helpdesk.
- 6.1.5. Users should report suspected infections of viruses to the Helpdesk and provide all known information about the virus or incident including what was done to make the user think they got a virus and what messages were received from the computer system or software at the time of the incident.
- 6.1.6. Users are not allowed to disable anti-virus software.

## **6.2. Installation of Detection Software on PCs**

- 6.2.1. ITS ensures that software is installed on each personal computing device (PC) and ensures that the software is updated as needed.

## **6.3. Remediation and Corrective Action**

- 6.3.1. ITS remediates and takes corrective action upon identification of a virus or malware.

#### **6.4. Reasonable and Necessary Accommodations**

- 6.4.1. Management may take reasonable and necessary actions to accomplish the intent of this policy.