Category: ITS Policy Policy No.: ITS-08-2024 Revisions: February 7, 2024	middlesex centre in the centre of it all	Pages: 5 Effective Date: Feb 7, 2024 Report No.: CPS-06-2024

Malware Protection

Purpose

The purpose of this policy is to outline the implementation and configuration of endpoint protection tools, user security awareness, early detection and mitigation security systems and ensure staff are aware of security policies in place on their IT assets.

Scope

This policy applies to Members of Council, all employees of Middlesex Centre including Paid-on-Call Firefighters and volunteers.

Definitions

"(ITS) Asset" means any physical electronic device owned by Middlesex Centre, which may contain or have access to sensitive information such as files and emails or has considerable value and is uniquely identifiable via a serial number.

"Endpoint" any device which connects to a computer network, such as a server, workstation, or laptop.

"Grayware" is a potentially unwanted program (PUP), which is not obviously malicious and is not classified as a virus but can still be irritating or harmful. Common forms of grayware include Adware and Spyware.

"ITS" means Information Technology Services.

“Macro” is a series of computer commands that are stored and run to automate a computer task.

"Malware" is catch-all term for software which is designed to disrupt, damage, or gain unauthorized access to a computer system.

"Middlesex County ITS" is the department at Middlesex County responsible for procurement, maintenance, and support of Information Systems.

“Principle of Least Privilege” is an information security approach whereby users are given the minimum level access / permissions required to perform their job duties.

Responsibilities

Middlesex Centre employees shall ensure:

a) Staff are aware of the security policies enforced on their workstations

b) Staff report all incidents to Middlesex County ITS

c) Staff shall not modify, disable, or tamper with Middlesex County ITS installed tools

Middlesex County ITS shall ensure:

a) Procedures and tools exist to guard against, detect, and report malicious software

b) Middlesex County ITS personnel are trained and proficient in the use of the security solutions used to protect against malicious software

c) Staff are aware of the security policies enforced on their workstations

Procedure

1. Antivirus Software / Endpoint Protection Tools

Antivirus/Endpoint Protection Tools shall be configured according to best practices as defined by the software vendor, including:

a) Any ITS workstation, laptop, and server supported by Middlesex County ITS capable of running an approved Antivirus/Endpoint Protection Tool shall have one installed.

b) Antivirus/Endpoint Protection Tools shall be configured to receive regular malware definition updates.

c) All Antivirus/Endpoint Protection Tools shall be configured to automatically scan files for potential security threats as they are created, accessed, modified, and deleted.

d) Supported systems shall be configured to automatically perform a full scan of a device on a scheduled basis.

Staff shall not modify, disable, or tamper with Middlesex County ITS installed Antivirus/Endpoint Protection Tools.

2. Adaptive Defense and Quarantined Applications

Middlesex County ITS approved Antivirus/Endpoint Protection Tools operate using a concept known as adaptive defense. Adaptive defense allows these tools to identify threats as they occur without any prior knowledge of the threat itself.

Should an unknown software application be run on an ITS Asset, it may be automatically quarantined by the Antivirus/Endpoint Protection Tool. These quarantined applications are subject to review by Middlesex County ITS prior to them being allowed to run on an ITS Asset.

Additionally, adaptive defense allows an Antivirus/Endpoint Protection Tool to identify common actions or behaviors conducted on an ITS Asset. Should the behaviours become atypical, the system may flag them for review or prevent further action from being taken on the ITS Asset. Systems or services until such time as Middlesex County ITS reviews to determine if the potential threat is legitimate.

3. System Quarantine

In accordance with the Middlesex County Incident Response Plan:

a) Should an ITS Asset be identified as infected with a threat including but not limited to; a virus, malware, trojan or ransomware, the ITS asset may be quarantined from the network, with all connectivity restricted.

b) ITS Assets quarantined in this manner will not be recoverable, including any saved or unsaved files stored on the ITS Asset.

c) In extreme cases, Middlesex County ITS may deem the ITS Asset unfit for purpose and recommend its disposal, destruction, and replacement.

4. Unsupported Critical Devices and Systems

Devices and/or systems which are required to provide critical Middlesex Centre functions which are not capable of running an Approved Antivirus/Endpoint Protection tools shall:

a) Have best-effort Antivirus/Endpoint protection tools (such as an older version or a protection tool from an alternate vendor) installed and enabled, and;

b) Be replaced or upgraded as soon as reasonably possible, with a timeline to be determined through discussion of Middlesex County ITS and the department director for which the function or service is performed, and;

c) Remain isolated from other systems or services except for systems or services which are required for the Unsupported Critical Device to function.

5. Least Privilege

To mitigate potential spread during an incident, all staff accounts shall be configured according to the principle of least privilege.

6. Email Attachment Restriction

All inbound email messages to sites supported by Middlesex County ITS are subject to automatic scanning for malicious links or attachments.

Emails which contain potentially malicious links or attachments are automatically quarantined for further review. Should the quarantined email later be determined to be legitimate, it can be released to the intended recipient.

7. Macros and Scripting/Automation

Documents capable of performing automatic actions using scripting or macros shall be subject to review by Middlesex County ITS prior to their use.

Productivity suites which support the use of these scripts or macros shall be configured to automatically prevent their use until action is taken to explicitly trust the document containing such script or macro, with approval from Middlesex County ITS.

8. Software Installation and Security Assessments

All software, extensions, or applications installed on Middlesex Centre's computer systems shall be installed by Middlesex County ITS staff or a Middlesex County ITS approved third-party software vendor.

Middlesex County ITS may conduct security assessments on any software, extension or application requested by staff prior to their installation.

9. USBs and Other External Drives

Extra care should be taken with the use of USBs and other external drives. In general, external drives should be avoided whenever possible. If an external drive is required, only those purchased by the municipality should be used. Under no circumstance should drives from meetings, conferences, salespeople, etc. be used with Middlesex Centre hardware.

10. Training and Education

Middlesex Centre conducts training automated phishing campaigns. These campaigns are intended to foster staff awareness of potential cyber-security threats and the methods in which they may be distributed.

Middlesex Centre encourages all staff who may be uncertain if an email, website or file is suspicious to contact the Middlesex County Service Desk for further assistance.

Security awareness training is provided to staff by Middlesex Centre using third-party vendors and support tools in collaboration with Middlesex County ITS.

11. Compliance

Corporate Services and Middlesex County ITS enforce this policy and related standards. Anyone who has reason to suspect a deliberate and/or significant violation of this policy is encouraged to promptly report it to the Middlesex County ITS Service Desk. Policy violations that come to the attention of the ITS Service Desk will be escalated to the Director of ITS and Director of Corporate Services.

Staff in violation of this policy may be subject to disciplinary action up to and including termination.

Policy Review

This policy will be reviewed once every four (4) years, or as necessary.