


CHAPTER: 10	SECTION: 10	SUBJECT: MANAGEMENT OF INFORMATION
TITLE: ANTI-VIRUS AND ANTI-MALWARE		
EFFECTIVE DATE: 09/26/17	REVISED DATE: 04/12/19, 6/3/20, 05/06/21, 10/20/22, 11/14/23	
ISSUED AND APPROVED BY:    EXECUTIVE DIRECTOR		

**I. PURPOSE**

To establish policy and procedure for the protection of the networked environment through use of anti-virus and anti-malware software.

**II. APPLICATION**

All county-owned hardware, including laptops, desktops, and cell phones, utilized by employees that present a potential breach point for confidential information.

**III. DEFINITIONS**

**Anti-Virus Software (AV):** Software that provides an electronic defense mechanism mitigating or reducing the risk of a networked device being infected with or affected by malware.

**End Points:** All devices within a networked system capable of being affected or infected by malware.

**Malware:** A term used to generally refer to a variety of forms of hostile or intrusive software typically meant to disable or damage computers and computer systems.

**Phishing:** The practice of sending fraudulent emails purporting to be from reputable companies or familiar individuals meant to induce the recipient into revealing personal information, such as passwords or credit card numbers.

**Social Engineering:** A technique used by attackers to attempt to subvert security controls by attempting to convince a legitimate user to divulge sensitive information, including passwords, IP addresses or details of security mechanisms in use, or to install and run inappropriate malware.

**Spam:** An unsolicited email received from an unrequested source which attempts to convince the recipient to perform an identified action, which is often purchasing goods or services via a provided link.

**Virus:** A computer program that can copy itself without permission or knowledge of the user, which typically has a detrimental effect, such as corrupting a system or network or destroying or accessing data.

**IV. POLICY**

It is the policy of Community Mental Health of Ottawa County (CMHOC) to ensure confidentiality of personal records of both staff and consumers. CMHOC recognizes the responsibility inherent in holding personal and will work with Ottawa County IT to implement and engage various software protections to mitigate potential threats.

**V. PROCEDURE**

- A. All end points and network entry points are protected from virus, malware, and other potentially harmful programs that may or have the potential to compromise data or cause damage to the whole or any part of the networked environment. This is managed through the utilization of:
- a. Cisco FirePower appliances in high availability at our two internet connections.
  - b. Cisco Secure Email (FNA IronPort)
  - c. Cisco Umbrella - uses the Internet's infrastructure to enforce security and block malicious activity before a connection is ever established. DNS-layer security
  - d. Sophos Central Device Encryption
  - e. Cisco Secure Endpoint - EDR (endpoint detection and response)
  - f. Blumira SIEM – XDR (extended detection and response)
- B. All staff receive annual Security Awareness Training in identifying and mitigating potential threats of Phishing or Social Engineering.
- C. All software installed on county-owned hardware must be done so within the strict limitations of the licensing agreement. No software from personal sources is to be installed on County-owned equipment, including Freeware and Shareware, unless prior authorization is obtained from the Director of the IT Department.
- D. To minimize the risk of cross-infection between networked and standalone equipment, the use of USB flash drives (“thumb drives”) is not permitted without prior authorization from the IT Department.

**VI. ATTACHMENT**

Not Applicable

**VII. REFERENCE**

CMH IT Strategic Technology Plan **2023-2025**  
Ottawa County Policy, Acceptable Use  
Ottawa County Policy, Electronic Communications  
Ottawa County Policy, Information Security

Ottawa County Policy, Internet Use

Ottawa County Policy, Remote Access and Application Service Provider (ASP)