SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **MALWARE DEFENSE**	Policy 8.24

I. POLICY STATEMENT

Malware is one of the most common threats facing Southwestern Community College. 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 the spread, or control the execution of malicious software or code.

To support this Safeguard, it is important for an enterprise to develop a holistic approach to defending against malware. This approach should include deploying appropriate malware defenses for the variety of assets deployed in the enterprise, properly configuring anti-malware applications, and managing these applications.

II. PROCEDURES

See SCC Procedure 8.24.01 (MALWARE DEFENSE).

Adopted: September 2025

Revised: N/A