SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **SECURE CONFIGURATIONS MANAGEMENT**	Policy 8.21

I. POLICY STATEMENT

Southwestern Community College's ("College") enterprise assets are often not set up by default in the most secure configuration. This is often done to provide flexibility for our customers to apply their own secure configurations in accordance with their own security policies, but also to ensure the product functions "out of the box". Therefore, the presence of default accounts or passwords, excessive access, or unnecessary services are common in default configurations. These could introduce weaknesses that are under the responsibility of the enterprise using the asset. Even after a strong initial configuration is developed and applied, it must be continually managed to avoid degrading security as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked," to allow the installation of new software or to support new operational requirements.

There are a variety of enterprise, software, and other assets and services that may require configuration. These include hardware, software, and third-party services. Common examples include:

- **Operating system configuration:** This includes modifying the settings for the common operating systems such as Microsoft® Windows, Apple® MacOS, and the various flavors of Linux® and Unix. Smartphones, tablets, wearables, and Internet of Things (IoT) devices may all be configurable to various extents.

- **Applications:** Software written for any platform may require configuration. This includes software written for laptops, servers, smartphones, tablets, wearables, and IoT devices. Databases, hypervisors, and virtual machines may also be included.

- **Cloud services and platforms:** Third-party service providers may provide entire platforms that can be configured. These platforms may also provide individual applications that may be configured.

- **Network appliances:** These all-in-one physical boxes aid in the flow to network connected devices. These include routers, switches, firewalls, and wireless access points (WAPs).

II. PROCEDURES

See SCC Procedure 8.21.01 (SECURE CONFIGURATIONS MANAGEMENT).

Adopted: September 2025

Revised: N/A