SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **DATA RECOVERY**	Policy 8.25

I. POLICY STATEMENT

At Southwestern Community College ("College"), besides user education and antivirus software, one of the best ways to recover from the impact of ransomware is backing up data to another system before there is a problem. But backups alone would not completely prevent this malware from accomplishing its goals. Typical backups may be connected to another system or network, meaning backup data can still be attacked. Therefore, regular backups should be stored in an unconnected, off-the-network, manner. Keeping offline backups helps enterprises recover and restore systems when ransomware or destructive malware hits a system. A common way for this malware to get into a network is to be installed via email attachments or drive-by downloads from websites. Both of these types of malware have impacted law enforcement, hospitals, governments, and academic institutions and cost millions of dollars to recover. Leveraging the guidance within the CIS Controls will help reduce the risk of ransomware through improved cyber hygiene, as attackers usually use older or basic exploits on insecure systems.

II. PROCEDURES

See SCC Procedure 8.25.01 DATA RECOVERY.

Adopted: September 2025

Revised: N/A