SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **END USER INFORMATION SECURITY**	Procedure 8.14.01

I. SCOPE

This policy applies to all College faculty, staff, and students, whether full- or part-time, paid or unpaid, temporary or permanent, volunteers, as well as to all other members of the College community.

II. DEFINITIONS

A. **Availability:** The degree to which information and critical College services are accessible for use when required.
B. **Confidentiality:** The degree to which confidential College information is protected from unauthorized disclosure.
C. **End User or User:** The person or organization that actually uses a product, as opposed to the person or organization that authorizes, orders, procures, or pays for it. End Users include students, faculty, staff, contractors, consultants, and temporary employees.
D. **End User Device:** A device used by a member of the College community to accomplish access to information technology resources, including PCs, laptops, tablets, or smartphones.
E. **Information Resource:** Data, information, and information systems used by College to conduct College operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.
F. **Information Security:** The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability of data.
G. **Integrity:** The degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the College.
H. **Risk:** A probability or threat of damage, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.
I. Security Incident: An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information system operation; or violation of information security policy.

III. END USER DEVICE SECURITY

- Protect access to all devices using strong passwords.
- Log off, lock, or shut down devices before leaving unattended.
- Enable a password protected auto-lock or automatic screensaver to activate after no more than 15 minutes of inactivity.
- Secure portable and mobile devices at all times – lock them up or carry them with you.
- Lock the device in a secure location (e.g. drawer, cabinet, office, room, trunk) if away for an extended period of time.

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **END USER INFORMATION SECURITY**	Procedure 8.14.01

IV. PASSWORDS

- Never share your password with another individual, including administrative assistants, graduate assistants, IT Services staff, co-workers, family, friends, etc. All passwords must be treated as confidential College information.
- Use longer passwords. Longer passwords are stronger passwords.
- Do not use passwords that refer to personal data (i.e. children's names or your birth date).
- Do not use passwords that contain dictionary words.
- Do not reveal a password on questionnaires or security forms.
- Do not use the "Remember Password" feature in Windows or applications (e.g. Google Chrome, Microsoft Edge, Firefox, etc.).
- Do not write passwords down and store them anywhere accessible by others.
- Do not type your password when someone is looking over your shoulder.
- If your password has been inadvertently compromised, change it immediately.

V. VIRUS AND MALWARE PROTECTION

- Employ anti-virus software and update the scanning engine and signature database on a regular basis.
- Do not open unexpected or suspicious attachments received in email.
- Configure applications (word processing, spreadsheets, etc.) to require user confirmation before macros, scripts, or other executables are opened or executed.
- Scan removable or portable media for viruses prior to using on any machine connected to the College network. Examples of removable or portable media devices include laptops, USB memory sticks, external Hard Disk Drives, CDs, DVDs, Compact Flash or SD memory cards, magnetic tapes, etc.

VI. DISTRIBUTION AND TRANSMISSION OF INFORMATION

Sensitive College information that is transmitted electronically, transported physically, or spoken in conversation must be appropriately protected from unauthorized interception. Please review College policy 8.11 Information Classification and Handling for specific requirements and policies regarding information handling.

VII. DESTRUCTION AND DISPOSAL OF INFORMATION AND DEVICES

Sensitive College information must be securely disposed of to ensure it cannot be retrieved and recovered by unauthorized persons. Please review College policy XXX Information Classification and Handling for specific requirements and policies regarding information handling.

VIII. INCIDENT REPORTING

All members of the College community are required to report suspected or actual information security incidents or security breaches. These incidents include thefts of computer devices, viruses, worms, or computer "attacks" that may lead to unauthorized access to confidential information.

Information security incidents should be reported to:

- Information Security Office / Officer, vickih@southwesterncc.edu.

- IT Help Desk, 828-339-4409 or ticket@southwesterncc.edu.
- College manager or supervisor.

IX. REVIEW AND REVISION

This policy will be reviewed annually or as new incident management practices and regulations emerge. Updates will incorporate lessons learned from incidents and advancements in cybersecurity techniques.

Legal References:

- North Carolina Statewide Information Security Manual, SCIO-SEC-308 - Incident Response
- FERPA (20 U.S.C. § 1232g)
- GLBA (15 U.S.C. § 6801)
- NIST SP 800-61: Computer Security Incident Handling Guide

Cross References:

- Policy 8.08 – Account and Credential Management
- Policy 8.10 – Information Security Program
- Policy 8.24 – Malware Defense

Adopted: September 2025

Revised: N/A