SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **HUMAN RESOURCE SECURITY**	Procedure 8.12.01

I. SCOPE

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

II. ACRONYMS/DEFINITIONS

Availability - The degree to which information and critical College services are accessible for use when required.

Confidentiality - The degree to which confidential College information is protected from unauthorized disclosure.

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.

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.

Integrity - The degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the College.

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**.**

III. PROCEDURE

A. WORKFORCE SECURITY PRIOR TO EMPLOYMENT

Employees will screen as addressed in HR Policy 4.01.02 - Employment and Hiring.

B. WORKFORCE SECURITY DURING EMPLOYMENT

All College employees must read and acknowledge *Policy 8.02 - Acceptable Use* and other College information security policies upon the start of their employment with the College. Training and education on the information security policies will be conducted/coordinated periodically by the College Information Security Office/Officer (ISO). New employees will have the opportunity to attend these training sessions as they are held.

The College will define and explain security responsibilities for the role played by the employee and make clear the ramifications of failing to comply with College policies. Employees must be provided sufficient training and supporting reference materials, and are expected to apply this training, to properly protect College information resources.

Employees changing roles may need to receive additional security review and training before beginning a new role with more stringent security requirements. Department management and/or Human Resources staff must ensure access rights have been revoked/adjusted appropriately when an individual changes roles.

C. WORKFORCE SECURITY FOR TERMINATED EMPLOYMENT

When an individual's employment with College terminates, the College will ensure:

- All access accounts are disabled within twenty-four (24) hours of the termination action.
- Exit interviews are conducted, if possible and appropriate.
- All College information resource-related property is recovered.
- All College-owned information the terminated employee was responsible for is identified and accounted for.
- All College equipment is collected, such as laptops, laptop chargers, mobile devices, mobile device chargers, physical keys, identification badges, and keycard badges.

When possible, separation activities are to be coordinated with the Information Technology Division (IT) in advance. If advance coordination is not possible, then department management and/or Human Resources staff must engage IT immediately to revoke or adjust access rights.

Upon termination of an individual deemed to be a risk to the College, HR is required to immediately notify the ISO and IT to revoke the individual's IDs, privileges, and authorizations without delay.

D. DISCIPLINARY PROCESS

Individuals found to be in violation of policy will face disciplinary action. College will consider the severity, impact, and other relevant factors of the violation(s) in determining the extent of discipline. Where a violation of non-compliance of information security policy has occurred, corrective actions and sanctions available to the College include, but are not limited to:

- Restriction or suspension of computer access privileges.
- Disciplinary action by their academic division and/or the College up to and including termination/expulsion.
- Referral to law enforcement authorities for criminal prosecution.
- Other legal action, including action to recover civil damages and penalties.

IV. CONFIDENTIALITY AGREEMENT

College employees are required to protect the College's confidential information in accordance with this and other College policies at all times.

Certain employees may be required to sign a confidentiality agreement as a condition of employment.

Confidentiality agreements will be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving the organization.

V. SANCTIONS/ENFORCEMENT

Any College faculty, staff, or student found to have violated this policy may be subject to disciplinary action. Sanctions will be proportionate with the severity and/or frequency of the offense and may include termination of employment or expulsion. In addition, violators may be subject to criminal and/or civil action.

VI. EXCEPTIONS

No approved exceptions exist at this time.

Legal References

- N/A

Cross References

- Policy 4.01.02 - Employment and Hiring

Adopted: September 2025

Revised: