SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **ACCESS CONTROL**	Procedure 8.16.01

I. SCOPE

This policy applies to all College employees, contractors, students, and any other individuals who require access to the College's information systems. It covers all access to network resources, databases, applications, and any other systems that store or process College data.

II. DEFINITIONS

A. **Access Control:** The process of granting or denying specific requests to obtain and use information and related information processing services.
B. **Least Privilege:** The principle that users should be granted the minimum level of access, or permissions, necessary to perform their job functions.
C. **Authentication:** The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
D. **Authorization:** The process of granting or denying access rights to a system, service, or data based on the user's role and permissions.

III. RESPONSIBILITIES

A. **Information Security Officer (ISO):** The ISO is responsible for overseeing the implementation and management of access controls and ensuring compliance with this policy.
B. **System Administrators:** System Administrators are responsible for configuring, maintaining, and auditing access controls on the systems they manage.
C. **Users:** Users are responsible for maintaining the confidentiality of their access credentials and adhering to the access control protocols defined in this policy.

IV. ACCESS CONTROL REQUIREMENTS

A. **User Identification and Authentication:**
    1. All user accounts must be uniquely identified and authenticated through an approved method before accessing the College’s information systems.
    2. Multi-factor authentication (MFA) is required for accounts accessing sensitive or confidential information.
B. **Role-Based Access Control (RBAC) and Privilege Management:**
    1. Users are assigned roles based on job functions, aligned with the principle of least privilege.
    2. Access rights must be reviewed annually for all users and semi-annually for privileged accounts.
    3. Changes in job responsibilities must be reflected in the user’s access rights within 5 business days.
    4. Accounts with elevated privileges or access to critical systems must be closely monitored. Any high-risk accounts must be disabled immediately upon detection of security threats.
C. **Account Management and Monitoring:**
    1. Accounts inactive for 90 days must be automatically disabled. Disabled accounts remaining inactive for 365 days must be deleted unless required for records management or other legal purposes.

2. Temporary and emergency accounts must be pre-authorized, have a specific expiration date, and be removed promptly when no longer needed.
3. Automated systems will log all account creation, modification, and deletion activities. Monthly audits of these logs must be conducted to detect any unauthorized access attempts, with discrepancies reported to the ISO.

D. **Mobile and Remote Device Access:**

1. All mobile and remote devices accessing College systems must use encryption and MFA.
2. Non-compliant devices will be denied access until compliance is verified.
3. Remote access sessions will be regularly monitored for unauthorized activity. Daily reports of remote access logs will be reviewed for any suspicious actions.

V. ENFORCEMENT

Violations of this policy may result in disciplinary action, up to and including termination of employment or academic sanctions. Unauthorized access to College information systems is also subject to civil and criminal penalties under applicable laws.

VI. REVIEW AND REVISION

This policy will be reviewed annually or as needed to ensure its alignment with evolving security practices and regulatory requirements.

Legal References

- Statewide Information Security Manual, NC Department of Information Technology, SCIO-SEC-301: Access Control Policy (AC)
- CIS Controls v8, Control 6 (Access Control Management)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations
- 1B SBCCC 700.3 - Community College System Cybersecurity Framework

Adopted: September 2025

Revised: N/A