


|   |   |                                    |                |                               |  |
|---|---|------------------------------------|----------------|-------------------------------|--|
| <br><b>SOUTHEAST MISSOURI</b><br>STATE UNIVERSITY · 1873 | <b>BUSINESS<br/>         POLICY<br/>         AND<br/>         PROCEDURE<br/>         MANUAL</b> | Date Issued:<br>8/22               | Revision Date: | Page:<br>1 of 2               |  |
|   |   |                                    |                | Classification Code:<br>10-15 |  |
|   |   | Section:<br>INFORMATION TECHNOLOGY |                |                               |  |
|   |   | Subject:<br>LEAST PRIVILEGE POLICY |                |                               |  |

**PURPOSE:**

The purpose of this policy is to ensure the security of Southeast Missouri State University's data and systems by implementing the principle of least privilege and separation of duties. This policy outlines the responsibilities of faculty, staff, and administrators in maintaining secure access to data and services.

**POLICY STATEMENT:**

Southeast Missouri State University requires all faculty, staff, and administrators to follow the principle of least privilege, which ensures that each user has only the minimum necessary permissions to perform their job responsibilities. Supervisors must regularly review their staff's access to data and services and ensure that permissions are set at the lowest required level.

**DEFINITIONS**

**Principle of least privilege:** A user, program, or process should have only the minimum necessary permissions to perform a function.

**Separation of duties:** The requirement for more than one person to complete a specific task to prevent theft or misuse of resources.

**Local Administrator Account:** A non-domain account with full access to directories, files, services, and other resources on a local computer.


**Role-Based Access Controls (RBAC):** Limits data or network access based on an employee's or user's specific roles or responsibilities.

**Security Information Events Management (SIEM):** An information security tool that stores and maintains important log files and provides real-time analysis of security alerts generated by applications and network hardware.

**SCOPE OF POLICY**

This policy applies to all services and data within Southeast Missouri State University and mandates the following:

1. Southeast Missouri State University implements a Role-Based/Privilege-Based framework for all services and data, setting user permissions at the lowest necessary level for job functions.

|   |   |                                    |                |                               |
|---|---|------------------------------------|----------------|-------------------------------|
| <br><b>SOUTHEAST MISSOURI</b><br>STATE UNIVERSITY · 1873 | <b>BUSINESS<br/>         POLICY<br/>         AND<br/>         PROCEDURE<br/>         MANUAL</b> | Date Issued:<br>8/22               | Revision Date: | Page:<br>2 of 2               |
|   |   |                                    |                | Classification Code:<br>10-15 |
|   |   | Section:<br>INFORMATION TECHNOLOGY |                |                               |
|   |   | Subject:<br>LEAST PRIVILEGE POLICY |                |                               |

2. The University manages University-provided devices, including determining software installation, data access, and user login permissions.
3. Each college, department, division, or organization is responsible for limiting staff access to data and services based on job responsibilities.
4. Elevated permissions are granted only when needed and must be removed once the task is complete or the permissions are no longer required.
5. A centralized log collection application or SIEM must be used to maintain and monitor all relevant logs for all systems or applications and track inappropriate access to data or devices.
6. New applications or services, including in-house, commercial, or cloud-based, must provide role-based access to data.
7. The Assistant Vice President of Information Technology will address exceptions to this policy on a case-by-case basis.