Technology Solutions – System and Application Access Management

Department: Technology Solutions
Procedure Name: System and Application Access Management
Procedure ID: TS-PROC-008
Effective Date: 01/21/2026
Last Reviewed: 01/21/2026

Owner: Chief Information Officer (CIO)

Applies To: All Technology Solutions staff and leadership

1. Purpose

The purpose of this procedure is to establish clear, secure, and consistent standards for granting, managing, and reviewing system and application access within Technology Solutions to protect institutional assets, ensure accountability, and align with cybersecurity best practices.

2. Scope

This procedure applies to endpoints, servers, infrastructure systems, applications, administrative access, and both on-premises and cloud environments. It applies to all Technology Solutions staff, contractors, and temporary personnel.

3. Roles & Responsibilities

Role	Responsibility
CIO	Final approval authority for elevated and administrative access
Directors / Managers	Request access and provide business justification
System Owners	Ensure role-based access is enforced
Staff	Use access appropriately and report access issues
Security / I&O	Enforce technical controls and monitoring

4. Access Management Principles

- Least Privilege – Users receive only the access required to perform their job
- Role-Based Access – Access is assigned based on role, not individual preference

- Single Sign-On (SSO) First – Centralized authentication is the default
- Auditability – Access decisions must be traceable and reviewable

5. Endpoint Administrative Access

5.1 Local Administrator Access

Technology Solutions staff will not be granted local administrator rights on endpoints by default. Local administrator access may be granted only with CIO approval. Requests must originate from the staff member's manager, include clear business justification, and define duration if temporary.

5.2 Elevated Access via LAPS

When elevated access is required on an endpoint, Local Administrator Password Solution (LAPS) must be used. Shared or static local administrator passwords are prohibited. LAPS-managed credentials must be rotated automatically and logged.

6. System and Application Access

6.1 Role-Based Access Control (RBAC)

All systems and applications must use role-based access control where supported. Access must align with the individual's job responsibilities. Ad-hoc access outside defined roles should be avoided.

6.2 Single Sign-On (SSO)

Single Sign-On is the preferred authentication method for all supported systems. New systems must integrate with institutional identity services where feasible. Local accounts should be used only when SSO is not technically supported.

7. Elevated and Privileged Access

Administrative or privileged access requires CIO approval, must be justified by job function, and must be reviewed periodically. Privileged access must not be used for day-to-day activities where non-privileged access is sufficient.

8. Access Requests & Changes

All access requests must be approved by the staff member's manager, reviewed by the system owner, and documented. Access must be modified promptly when job roles change and removed immediately upon separation or termination.

9. Access Reviews

Periodic access reviews must be conducted to validate continued need, identify excessive or unused access, and ensure alignment with current roles. Findings must be documented and remediated.

10. Monitoring & Accountability

Administrative and privileged access may be monitored and logged. Users are accountable for actions performed using their credentials. Credential sharing is prohibited.

11. Exceptions

Exceptions require explicit CIO approval and must be documented, including justification, scope, duration, and compensating controls.

12. Compliance

Failure to follow this procedure may result in access revocation, security review, or corrective action. This procedure is governed under TS-PROC-001.

13. Review Cycle

This procedure will be reviewed annually or as security, operational, or institutional needs change.