Committee Meeting: Policy & Governance Committee	Date: January 12, 2026
Committee Chair: Melodie Baker	
New or Edited: New	

POLICY NAME: Access Management Policy

POLICY TYPE: Managerial

SUBMITTED BY: Daniel Bartkowiak, Information Security Officer

ISSUE OR STATEMENT OF PURPOSE: The purpose of this Access Management Policy is to establish a structured, auditable, and secure framework for managing access to SUNY Erie's information systems and data. This policy ensures compliance with SUNY Policy 6900 Section 6 and supports the principles outlined in the SUNY Erie Information Security Policy (ISP), specifically Section 5.1 Access Control.

NEW OR EDITED POLICY: New

POLICY:

Scope:

This policy applies to all SUNY Erie workforce members, including employees, contractors, consultants, vendors, and any other individuals or entities with access to the College's systems, data, or facilities, including but not limited to Active Directory (AD), Workday, email, network resources, and enterprise applications.

Policy Objectives:

- Ensure access is granted based on the principle of least privilege.
- Coordinate with Human Resources and the Human Capital Management (HCM) system to ensure account lifecycle activities are accurately reflected in access management processes.
- Enforce strong authentication mechanisms including Multi-Factor Authentication (MFA).
- Maintain auditability and accountability for all access-related actions.
- Protect sensitive institutional data from unauthorized access.

Account Types:

- User Accounts: Assigned to individuals for daily operations.
- Privileged Accounts: Used for administrative tasks with elevated permissions.
- Service Accounts: Used by applications or systems to perform automated tasks.
- Shared Accounts: Used by multiple authorized individuals for specific operational needs when individual accounts are impractical.

Account Creation:

- Accounts are provisioned based on identity and role via Workday. AD accounts are synchronized with Workday attributes.

Account Modification:

- Changes to accounts occur in response to role or employment changes:
- Employee Accounts: Changes in the Human Capital Management (HCM) system trigger access reviews and updates. During the "Change Job" business process, assignable roles are automatically removed and must be manually reassigned after completion. Human Resources coordinates these updates, and ITS applies changes through service desk tickets.
- Student accounts are not subject to change reviews unless the student is also an employee.
- Vendor and affiliate accounts (e.g., ASC and ECC Foundation) manage their own access changes and submit tickets to ITS as needed.
- Other third-party accounts are generally outside the scope of automated monitoring for modifications; however, Workday implementer accounts are automatically deactivated after a defined inactivity period.

Account Disablement:
Accounts are disabled in accordance with employment status, contractual obligations, or account ownership:

- Employee Accounts: Disabled 30 days after separation, suspension, or termination to allow completion of Human Capital Management (HCM) tasks, such as paystub access. Updates are managed through the HCM "Terminated Business Process." For retirees who return, accounts may be reactivated.
- Student Accounts: Access is limited after enrollment ends; accounts are deactivated one year after the last registered class. Non-registered students are not automatically disabled but may have access reviewed as needed.
- Vendor and Contractor Accounts: Disabled or set to expire based on estimated work completion. Vendors and affiliates, including ASC and ECC Foundation, are responsible for initiating account disablement via ITS tickets and must verify active engagement or employment at least biannually.
- General: Access is not granted once accounts are disabled. Specific data elements may be retrieved in accordance with institutional policies and procedures.

Account Deletion:
Accounts are deleted in accordance with HR and ITS retention schedules:

- Employee Accounts: Deleted 50 days after separation, following the 30-day disablement period.
- Student Accounts: Deleted two years after the last registered class, with account reviews and deletions conducted bi-annually.
- Vendor and Affiliate Accounts (e.g., ASC, ECC Foundation): Reviewed and deleted bi-annually.
- Workday Implementer Accounts: Expired accounts in Active Directory are deleted annually.

- Miscellaneous Third-Party Accounts: All third-party accounts should have an expiration date. Expired accounts are reviewed and deleted annually.

Employee Account Reviews:

- HCM/ERP Systems: Employee user accounts in the Human Capital Management (HCM) system and related ERP systems are reviewed semi-annually by ITS in coordination with the ERP Governance Team. Functional areas are responsible and accountable for reviewing accounts and ensuring the principle of least privilege is maintained. If functional areas cannot adjust access themselves, they must notify ITS to implement the necessary changes.
- Other Systems: Employee accounts in non-HCM/ERP systems are the responsibility of the respective functional areas. Functional areas are accountable for ensuring the principle of least privilege is maintained and must notify ITS of any required access changes.
- Reviews include verification of access appropriateness based on current roles and responsibilities.

Authentication:

- All accounts must use unique credentials.
- MFA is required for:
    1. Remote privileged access
    2. Privileged access for Workday
    3. Remote network access
    4. VPN access
    5. SUNY federated applications
    6. Institutional email
    7. SSO applications such as Office 365

Password Standards:

- Student accounts protected by MFA: Minimum 8 characters.
- All other accounts not protected by MFA: Minimum 14 characters.
- Passwords must not be reused across systems.
- Initial passwords must be changed upon first login.
- Accounts are locked after at most 10 failed login attempts.

Least Privilege:

- Authorization and privileges are granted strictly based on job function and business need.
- All authorization is granted solely for work-related activities. Accessing resources for non-work

purposes exceeds the scope of authorized use.

- Role-based access control (RBAC) is enforced via Workday roles and AD group memberships.

Access and Authorization Requests:

- All access and authorization requests must be submitted via the ITS ticketing system for approval by ITS.
- Requests require approval from the user's supervisor and data owner.
- All access is granted solely for work-related activities. Access is considered unauthorized if resources are used for non-work purposes.
- Temporary access must have defined expiration dates.

Access Reviews and Audits:

- ITS conducts regular audits of access permissions.
- Audit Logs: Retention of audit logs varies by system and is subject to existing technical capabilities. Logs must be retained long enough to support security monitoring, incident response, and compliance requirements. ITS is responsible for ensuring logs are available and reviewing opportunities to extend retention where feasible.
- Unauthorized Access Attempts: Access attempts identified through security alerts are investigated per the Incident Response Plan, with approved testing or proxy accounts excluded unless flagged as suspicious.

Shared Guest Accounts:

- User, privileged, and service accounts remain the property of SUNY Erie and must not be shared without explicit ITS approval.
- Shared accounts are discouraged and require documented justification and approval from the Information Security Program Lead (ISP).
- Guest accounts are temporary and must be approved by ITS administration and documented with reasoning and expiration dates.

Separation and Role Change:

- Employee user access is disabled according to the standard HR schedule for employee separations unless HR determines that immediate removal is required. In such cases, HR or the employee's supervisor must notify ITS without undue delay to implement the change.
- Role Changes: Changes to employee roles trigger access reviews to ensure permissions align with new responsibilities. Functional areas are responsible and accountable for reviewing and adjusting access in accordance with the principle of least privilege, particularly when the employee moves to a role with reduced access needs.
- Contingent Workers: Contingent workers are both vendors (ASC and the Foundation) and internships. Contingent workers in the HCM system will be reviewed annually.

- Employees who are also Students (e.g., Student Ambassadors): Functional areas remain responsible and accountable for ensuring that permissions follow the principle of least privilege.
- Alumni and Emeritus status employees: Do not retain SUNY Erie email accounts.

Enforcement:
Violations of this policy may result in disciplinary action, including termination of access, employment consequences, and legal action. ITS reserves the right to restrict accounts and resources in accordance with the Incident Response Plan.

Responsibilities:

- Users: Responsible for safeguarding credentials and complying with access policies.
- Supervisors: Responsible for notifying ITS of security-sensitive departures, or other access-related needs.
- ITS: Manages account provisioning, access reviews, and enforcement.
- HR: Coordinates with ITS to ensure timely updates to Workday for accurate role-based access.

DOES IT SUPERCEDE A POLICY/WHICH ONE (if so, attach redline version):

POLICY & GOVERNANCE COMMITTEE RECOMMENDED ACTION:
Policy & Governance Committee recommends the Board of Trustees accept the Managerial policy under Committee Briefings, Policy and Governance Committee. This Policy supersedes all prior policies/procedures and practices related to Access Management Policy.

DATE OF BOARD ACCEPTANCE: January 29, 2026

POLICY & GOVERNANCE COMMITTEE TEAM FOLLOW-UP:
Following Trustee acceptance, this Managerial policy will be included in the SUNY Erie Community College Managerial Policy Manual.

INFORMATION/INPUT CONSIDERED DURING POLICY & GOVERNANCE COMMITTEE DELIBERATIONS:

1. SUNY Information Security Policy
2. SUNY Data Classification Standard
3. SUNY Cloud Security Policy
4. Acceptable Use Policy
5. Access Management Policy
6. Security Risk Management Policy

The Policy has been reviewed and discussed at the Policy & Governance Committee meeting of January 12, 2026.

History

Item:	**Date:**	**Explanation:**
Policy adopted	January 29, 2026	
Annual BOT Review/Reaffirmed		
Previously Reviewed and Extended		
Renamed		

SUNY Erie Cross References

Policy Name or Procedure:	**Where to find:**
Acceptable Use Policy	College Catalog