THE STATE UNIVERSITY OF NEW YORK

GUIDANCE FOR MANAGING USER ACCESS

SUNY Office of Risk Management & Compliance
SUNY Office of Internal Controls
SUNY Office of the Chief Information Security Officer

12-4-25

FINAL

Table of Contents

Why User Access Matters

Effective management of employee access to systems containing sensitive data (e.g., student records, personnel data, financial data, research data, health records, intellectual property, donor/alumni information, institutional analytics, etc.), is critical to the operations of every unit, campus, and SUNY.

User access is enforced by the **principle of least privilege**, which means granting users only the minimum level of access necessary to perform their job functions—nothing more. This helps to protect sensitive information, maintain operational efficiencies, limit opportunities for misuse (whether intentional or accidental), helps contain the impact of compromised accounts, and ensures compliance with SUNY policy and regulatory requirements. It is critical for protecting sensitive data and maintaining overall system security.

Definitions:

Provisioning:

Access provisioning is the administrative process of giving users the necessary permissions and access rights to perform their jobs within an organization's systems, applications, and data.

Modification:

Access modification after provisioning is a critical aspect of the employee life cycle, ensuring that users have the correct level of access throughout their time with a campus as roles and responsibilities change over time.

De-Provisioning:

Access deprovisioning is the process of removing a user's access to campus systems, applications, and data. This is done when a user leaves the campus, changes roles, or no longer needs access to certain resources. It involves revoking permissions, deactivating accounts, and retrieving campus assets to prevent security risks and maintain compliance.

Supervisor’s role in provisioning, modification, and de-provisioning:

Supervisors play a key role in accurately identifying the systems, applications, and data their employees need to perform their duties. They are responsible for ensuring access requests align with the employee’s job responsibilities and that the level of access granted follows the principle of least privilege. Supervisors should also verify that new employees complete any required training or compliance steps before access is granted. As employees take on new

responsibilities, transfer between departments, or experience changes in duties, supervisors must promptly review and update the employee's system access. When an employee separates from the campus or no longer requires access to certain systems, supervisors must ensure that de-provisioning actions are initiated immediately. This includes notifying the appropriate administrative or IT offices, confirming that all access has been removed, and ensuring that any University assets (e.g., equipment, ID cards, etc.) are returned. Supervisors should periodically review user access to confirm continued appropriateness and for communicating changes in a timely manner.

Failing to Manage User Access:

Failure to actively monitor and manage user access creates significant risks:

- **Operational Risks**: Outdated or excessive access can disrupt workflows, compromise data integrity, and create errors that affect students, faculty, and staff.
- **Financial Risks**: Inappropriate access and lack of segregation of duties increase the chance of waste, fraud, and abuse.
- **Compliance Risks**: FERPA, HIPAA, NIST, COSO, and other standards require strict controls. Non-compliance can lead to audit findings, penalties, and oversight.
- **Reputational Risks**: Security lapses damage trust among students, employees, partners, and the public.

Provisioning Guidance:

When creating new accounts, access must be provisioned strictly according to the user's current, validated, and documented business need. No access should be granted based on informal requests or assumptions. Each permission assigned should be reviewed in conjunction with the head of the department that owns the data to ensure it is the minimum necessary for the user to perform their job functions. If access is not necessary, explore alternate system access or BI Dashboards that provide only needed information without sensitive data.

Example: A new staff member is hired in the Registrar's Office. Before their account is created, HR confirms their official appointment and job duties. The IT team provisions access only to the student records system modules required for their specific

responsibilities. Access to financial or HR data is not granted unless a separate, documented business need is established and approved.

Example: A department requests that a new employee be given "the same access as their predecessor." Instead, IT reviews the new employee's job description and current business needs with the department, provisioning only the necessary permissions. Any additional access must be justified and approved, preventing legacy or unnecessary permissions from being carried over.

Risks of "Copy-Paste" Access

When granting system access, avoid the temptation to copy one employee's access to another (e.g., for a replacement hire). This shortcut creates vulnerabilities and inefficiencies.

1. **Violates Least Privilege** – May grant unnecessary or excessive permissions.
2. **Propagates Legacy Access** – Carries forward outdated or temporary permissions.
3. **Obscures User Clarity** – Undermines auditability and accountability.
4. **Creates Compliance Issues** – May violate FERPA, HIPAA, NIST, or COSO requirements.
5. **Reduces Efficiency** – Incorrect access can confuse employees and disrupt the ability to track access.

Deprovisioning Guidance

Failure to promptly remove access rights poses a **significant** cybersecurity risk. Upon separation, change, or end of assignment, all access rights must be promptly and completely removed. This includes not only primary accounts but also any secondary, system-specific, or legacy entitlements. When designing deprovisioning workflows, units should identify and specify which services are automatically disabled through Human Resource actions versus those requiring manual intervention.

Stale or misconfigured accounts are a common root cause of security breaches. A compromised network or identity system could allow a threat actor to exploit orphaned accounts and escalate privileges undetected.

Example: A staff member in the Registrar's Office retires at the end of the semester. On their last working day, HR notifies IT, which immediately rescinds their access to systems they no longer need, such as the learning management system, student information system, and email (See Appendix C). If the retiree is later rehired as a part-time employee, a new account is created with limited, time-bound access appropriate to the new role, rather than reactivating the old account.

Steps for Deprovisioning

1. **Initiate Notification**
    - Human Resources or Department Head should notify IT Security, Facilities, and relevant system administrators **no later than the employee's last working day**.
    - When internal users or functions change or when internal job transfers occur, identify which permissions should be removed or added and notify the appropriate security administrator for internal and external system permissions.
2. **Disable and Remove Access**
    - Submit requests for access deactivation.
    - Address local/system-specific requirements.
    - Immediately disable Single Sign-On (SSO) and identity credentials if leaving campus or if appropriate based on new role.
3. **Review Access Categories**
    - Applications and systems should be mapped to the correct owner (HR, ITS, Department, etc.) for removal.
    - Campuses/Units should supplement the checklist in Appendix A with additional categories as needed.

Key Takeaways

- Proactive monitoring and management of access protects SUNY's data, finances, and reputation.

- Every unit plays a role in provisioning, modifying, and deprovisioning access responsibly.
- Following these checklists ensures compliance with regulatory standards and safeguards the SUNY community.

Recommended Best Practices:

- Accounts should not be created or enabled until the user and business need are validated through authoritative sources (e.g., receiving a formal request for access from the HR department or the business unit).
- Document user access (Appendix B – User Access Justification Checklist)
- Review on a regular basis (recommend annually or anytime responsibilities change) the privileges assigned to users with access to sensitive data or operational systems (e.g., HR, finance, student data) to validate the need for such privileges; and reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs (Appendix B – User Security Justification Checklist).
- Use a ticketing system (if available) to accurately track provisioning, modifications, and de-provisioning of user access.
    - If no ticketing system is available, some other method of documenting the provisioning, modifications, and de-provisioning of user access should be employed and accessible to multiple users (not stored on an individual's computer).
        - Example – A campus security user access form that supports all user access activities that must be maintained (with applicable approvals).
    - The records should be maintained and available for reference and audit purposes according to applicable records retention and disposition schedules.
- Use a provisioning, modification, deprovisioning checklist (maintain for audit purposes) (Appendix A).
- Continued access for transitional purposes should be explicitly documented, time-bound, and approved by the Information Security Officer.
- ITS should verify deactivation of accounts across systems within 48 hours.
- A quarterly audit should be conducted to detect and resolve stale or orphaned accounts.

Appendix A

Provisioning, Modification, and De-Provisioning Checklist

Provisioning, Modification, and De-Provisioning Checklist 12-4-25 FINAL (1).xlsx

Please note: Access to the Provisioning, Modification, and De-Provisioning Checklist will expire 90 days after being issued.

Please contact ormac@suny.edu for a copy or for access.

The Provisioning, Modification, and De-Provisioning Checklist has been provided as a guide and is not an exhaustive list. Additional categories can and should be included if applicable to your unit or campus. Applications can be moved to the appropriate area based on ownership. There are yes/no drop downs under Provision and De-Provision for all categories. They can be copied and applied to new items.

Appendix B

User Access Justification Checklist (Sample)

Employee: _____

Date: _____

Attach User Access Provisioning, Modification, and De-Provisioning Checklist to this review - Provisioning, Modification, and De-Provisioning Checklist 12-4-25 FINAL.xlsx

1. Business Need

- ❑ Does the access directly relate to the employee's **job responsibilities**?
- ❑ Is there a **documented business process** requiring this level of access?
- ❑ Has the employee's **supervisor approved** the access request?

2. Least Privilege Principle

- ❑ Is this the **minimum access** required to perform the job function?
- ❑ Can **more limited access** meet the need instead?
- ❑ Has access been separated from functions that could create a **conflict of interest** (e.g., initiating and approving the same transaction)?

3. Compliance & Risk Management

- ❑ Is access consistent with **federal, state, SUNY, and institutional policies**?
- ❑ Does it align with **FERPA, HIPAA, GLBA, or other applicable regulations**?
- ❑ Has the risk of **data exposure** or **fraud** been evaluated and mitigated?

4. Duration & Review

- ❑ Is this access **permanent, temporary, or project-based**?
- ❑ If temporary, is there an **end date** or expiration built into the system?
  - End Date: _____
- ❑ Has this access been flagged for **periodic review** during security audits?

5. Documentation & Transparency

- ❑ Is the **justification written and stored** in the access request system?

- ❑ Has the request been **logged for audit purposes**?
- ❑ Is there a record of the **reviewer/approver's decision**?

6. Separation of Duties

- ❑ Has a **Separation of Duties analysis** been completed?
- ❑ Could this user, in combination with others, create **fraud or compliance risks**?
- ❑ If exceptions are necessary, has a **mitigation plan (i.e., compensating controls)** been documented?

7. Modification or Removal of Security

- ❑ The following security should be **modified** or **removed**:

Supervisor Attestation:

I hereby attest that I have conducted a review of system access for this employee. I confirm that:

- ❑ **Business Need:** Current access is necessary for the employee to perform their assigned job responsibilities.
- ❑ **Least Privilege:** The employee has the minimum level required for job duties.
- ❑ **Separation of Duties:** Access has been reviewed to avoid conflicts of interest, and any exceptions have been documented and mitigated.
- ❑ **Compliance:** The access complies with all applicable institutional policies, federal and state regulations.
- ❑ **Review & Monitoring:** Access has been reviewed in support of ongoing appropriateness.

Supervisor Name: _____

Signature: _____

Date: _____

Appendix C

Emeritus Faculty and Alumni Accounts

On June 4, 2025, System Administration issued guidance on the management of SUNY emeritus and alumni accounts, addressing variability in campus interpretations of SUNY Board policy.

Emeritus accounts are digital privileges extended to retired faculty or administrative members in recognition of their distinguished service. However, providing on-going accounts to emeritus faculty and alumni creates risks by increasing the potential points of access to a campus network that a malicious cyber actor may be able to exploit. Every additional account introduces another possible access vector, which must be monitored and managed by campus Information Technology (IT) staff. Consequently, each additional account increases the institution's vulnerability to cyber threats and the administrative and operational workload of IT staff.

Campuses must incorporate cybersecurity concerns into their determination of which privileges are feasible to provide to retired faculty or administrative members, including the provision of campus accounts and access to campus digital resources. Campuses may restrict access to these resources, in whole or in part, based on the judgment of campus leadership.

Campuses should incorporate the use of least privilege when maintaining emeritus/alumni accounts and consider implementing compensating controls such as:

- Migrating emeritus/alumni accounts to a dedicated subdomain and retaining only messages which the individual requires on-going access to in their new status (e.g., for faculty/staff no on-going access to FERPA protected or HR-related records)
- Requiring emeritus staff and alumni who wish to maintain campus accounts to complete annual cybersecurity training.
- Implementing automatic password expiration for dormant accounts.
- Reviewing emeritus/staff accounts at regular intervals and disabling unused accounts.
- Developing a written policy outlining the conditions by which an emeritus/alumni account may be disabled due to user behavior.