SNOWBE ONLINE #010
SEPARATION OF DUTIES POLICY

Sean Redding

Privileged Access Policy -

Version # 1.0

10-12-25

Table of Contents

Purpose

The purpose of this policy is to establish protocols for managing Privileged Access to IT Resources, ensuring adherence to the Principle of Least Privilege, and promoting transparency, accountability, and security across SnowBe Online through thorough documentation, review, and auditing of access requests.

Scope

SnowBe Online 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

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

Roles & Responsibilities

Management:

Management is responsible for establishing and maintaining the control environment. Furthermore, periodic and routine review of preventive and detective controls is essential to have an effective internal control system.

Employees:

SnowBe Online employees play a role in strengthening SnowBe's internal control system. All employees of SnowBe Online should be aware of the concept and purpose of internal controls. They are responsible for understanding and following appropriate policies and procedures for their job. Employees must also notify supervisors of weaknesses in, and opportunities to enhance Internal Controls.

Policy

Management must consider the principle of segregation of duties when setting up new operational positions and defining job duties. Management must implement processes and control procedures that segregate duties among employees and that include effective oversight of activities and transactions.

The development of written departmental policies and procedures is an effective way to maintain a strong system of internal controls. Documented policies and procedures should be used to clearly delineate the control activities performed throughout the unit's various business processes. These will aid in the orientation of new employees, help ensure business continuity in the event of turnover, and help ensure compliance with applicable laws and regulations. It is every accounting department employee's duty and responsibility to bring areas of internal control weakness to the attention of the accounting department management for resolution. In an ideal environment, a different employee should perform each of the following major duties or functions.

Managerial Review

Management must make sure that no one person has the responsibility to complete two or more of these major functions. There is a greater need for proper segregation of duties for assets that are more liquid or negotiable (i.e., cash funds, negotiable checks, and inventories). Without additional Mitigating Controls in place, there is the potential to carry out and conceal errors and/or irregularities in the course of performing day-to-day activities.

Authorization

All transactions must be properly authorized. The individual initiating the transaction must have the authority to do so. Authorization confirms adherence to the following general requirements: Employees cannot authorize transactions for their own reimbursement; documentation of the Authorization must exist; all transactions must comply with SnowBe Online's policies, existing laws, regulations, compliance requirements, as well as any terms and conditions of the sponsor.

Recording

Recording is the process of creating and maintaining records of revenues, expenditures, assets, and liabilities. These may be manual records or records maintained in the Banner financial system.

Verification

Verification of processing or recording of transactions ensures all transactions are valid, comply with authorization requirements, and are properly recorded on a timely basis. This includes resolving identified differences or discrepancies. The verification must be documented with a signature (electronic or manual) and date.

Custody of Assets

Custody of Assets is the access to or control over physical assets such as cash, checks, equipment, supplies, or materials, and such assets are related to the incompatible duties to be segregated.

Managerial Review

In all cases, there is a level of review of the activity by management. This managerial review function assures that segregation exists and that the transactions are appropriate. The frequency and extent required of the managerial review depend upon the degree to which duties are or are not segregated.

Mitigating Controls

Several other control mechanisms may mitigate a lack of segregation of duties:
Audit trails enable the re-creation of the actual transaction flow from the point of origination to its existence on an updated file. Adequate audit trails should provide the initiator of the transaction, date and time of entry, type of entry, data fields, and files updated. Appropriate documentation must exist to support all transactions.

Reconciliation of applications and records increases the level of confidence that processes ran and/or interfaced successfully. When exception reports are presented to the supervisory level, supported by evidence, exceptions are reviewed, and when necessary, corrected timely. The review must be evidenced by the signature of the supervisor and dated. Managerial reviews should periodically be performed through observation, inquiry, and review of documentation to help detect errors and irregularities.

Exceptions/Exemptions

Requests for an exception must be submitted in writing to consult with the IT Director or IT Manager.

The request must be detailed with information, including:

- Length of time
- Policy or standard
- Reason

Each request will be reviewed by the IT Manager or IT Director to determine whether an exemption is justified and whether it will require compensating controls.

If the non-compliance is due to a better solution, an exception is still required and will be formally evaluated and approved.

The IT Director and the Commissioner must maintain constant communication during the exception. If approved, the Commissioner's office will send the letter of approval to the requester with details. In the event of denial, a letter of explanation will be sent to the requester with the reason the IT Director denied the request and an explanation.

Exemptions:

Access Control – Access controls, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), Sessions, and IAM policies, are not to be paused or discontinued.

Enforcement

- Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director.
- Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
- Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from SnowBe.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	10-12-25	IT Director	IT Director	Initial draft of policy.

Citations

https://semo.edu/finance-admin/_pdfs/finadm-10-15-policy.pdf

NIST Special Publication 800-53 Revision 5

https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment