Effective: *08/08/2022*
Last Revised: *08/08/2022*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

ITS-10: Personnel Security Standard

Standard Contents

1. Purpose

The purpose of the Personnel Security Standard is to define the organization's requirements for enforcing effective personnel management. This policy serves as a statement of objectives in the establishment of an effective security planning program in implementing best practices to personnel screening, termination, transfer, and management.

2. Scope

This Standard shall apply to all The University of Nebraska ("The University") personnel.

3. Standard Statement

It is the intention of this standard to establish best practices pertaining to personnel security. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer (CISO) as defined in **ITS Policy Exception Standard**. The following subsections outline the Personnel Security Standard.

4. Personnel Security Requirements

4.1 Personnel Screening

4.1.1 Personnel Screening Requirements

The University must screen non-student employees based on required level of access, prior to authorizing access to organizational systems which store or process medium or high-risk data as defined in Executive Memorandum 42. Background checks occur upon initial hire and when individuals change jobs, unless a background check has been conducted within the last 3 months.

4.1.2 Personnel Security Roles and Responsibilities

The University must establish and communicate personnel security roles and responsibilities for all employees and third-party contractors. Acknowledgement of roles and responsibilities must be included within access agreements and periodic security awareness training. Monitoring must be implemented to ensure ongoing compliance.

4.1.3 Access Agreements

University employees and contractors requiring access to organizational information and information assets must sign appropriate access (AUP) prior to access provisioning and at least annually. Access agreements must be reviewed and updated on an annual basis.

4.2 Personnel Terminations and Transfers

4.2.1 Personnel Termination

Upon termination of employment, all system and physical access must be terminated in accordance with the **Access, Identification and Authorization Standard**.

Where possible, exit interviews must be conducted to identify potential issues, problems or grievances that could affect future loss or security risk exposure and remind terminated individuals of nondisclosure agreements and potential limitations on future employment. Processes must be established to retrieve and retain all organizational property, such as IT hardware, keycards, and hard tokens from terminated personnel.

In certain circumstances, such as a reduction in force (or RIF), it may be appropriate for a terminated employee to retain access to certain systems such as email for up to 90 days.

4.2.2 Personnel Transfer
Employee Managers must review and update logical and physical access authorizations to information assets/facilities when personnel are promoted/demoted, reassigned, or transferred to other positions within the organization in accordance with the **Access, Identification and Authorization Standard**.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Exceptions
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	08/08/2022
Approved by:	Bret Blackman	IT CIO	08/08/2022

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published