Effective: *08/08/2022*
Last Revised: *03/12/2024*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
Director of Governance, Risk, and Compliance
its-sec@nebraska.edu

ITS-11: Physical Protection Standard

Standard Contents

1. Purpose

The purpose of the Physical Protection Standard is to define the organization's requirements for mitigating the risks from physical security threats through the establishment of an effective physical security and controls program. These physical security controls help The University of Nebraska protect its Information Technology Assets from physical and environmental threats. This standard outlines the methods and requirements for limiting physical access to authorized personnel.

2. Scope

This Standard shall apply to all University of Nebraska System ("University") technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of the University and to which this Standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this Standard.

3. Standard Statement

It is the intention of this Standard to establish consistent minimum standards for the physical protection of its Information Technology Assets and personnel. 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 Physical Protection Standard.

4. Physical Protection Requirements

4.1 General Physical Protection Requirements

4.1.1 Procedures and Responsibilities

Physical security procedures and responsibilities must be defined, documented, maintained, and disseminated to the applicable parties to which they apply.

4.1.2 Physical Access Authorizations

Access to office buildings, data centers, server rooms, networking closets, digital/physical data storage rooms, etc. where University networks, systems, and data are accessible must be physically restricted, and limited to users with job-related needs in accordance with the **Access, Identification and Authorization Standard**. Access controls may include manned reception areas, badge-controlled doors or turnstiles, key-locked doors, combination-locked doors, etc. Such doors must not be propped open or otherwise restricted from closing.

4.1.3 Infrastructure Access

Access to data centers, server rooms, networking closets, and other areas in which critical infrastructure is stored must be approved by the Chief Information Security Officer or Chief Information Officer and must be limited to those with a business justification.

Doors to such facilities must automatically close immediately after they have been opened and must trigger an alarm when they have been kept opened beyond a defined period of time. The doors must also be resistant to forcible entry.

4.1.4 Infrastructure Access Review

Access to data centers, server rooms, networking closets, and other areas in which critical infrastructure is stored must be reviewed by the Chief Information Security Officer on at least an annual basis.

4.1.5 Badge Access Management

All employees must always carry their university-issued badges on their person. Badges must be assigned to one individual only. Badges must never be shared with another individual to access company facilities. Loss of an assigned badge must be immediately reported to Campus ID Card Office. The lost badge must be immediately deactivated to prevent unauthorized use. If an individual forgets a badge, they shall be issued a temporary one-day badge after employment/contract status is verified with Campus Security.

Any change of status of any badge holder (termination of employment/contract, leave of absence, etc.) must be immediately reported to Human Resources and Campus Security to ensure physical access is properly disabled thereafter.

All physical badge accesses (University employees or third parties) must be logged and retained for at least twelve (12) months. All-access logs should be reviewed by the Chief Information Security Officer on a quarterly basis.

4.1.6 Tailgating

Personnel are forbidden from tailgating others to gain access to facilities that contain University information systems or data. Personnel witnessing tailgating are required to report the incident immediately to Campus Security.

4.1.7 Visitor Access

Visitors must check-in with a University representative upon arrival, wear a guest badge, and be escorted at all times while on the premises. The guest badge must have the date of the visit and must expire at the end of that day. These badges shall be clearly differentiable from assigned employee ID badges and must be returned at the end of the visit.

All physical accesses by visitors must be logged, with logs being retained for at least three (3) years. These logs must include the following:

- Name of the visitor
- Company represented by the visitor
- Purpose for their visit
- Date and time of arrival and departure.

4.1.8 Video Surveillance

Video cameras or other access control mechanisms (or both) must monitor the entry and exit points of rooms where sensitive systems or data are present. All physical access control mechanisms must be protected from tampering or disabling. Collected data from the cameras and other access controls must be stored for at least twelve months and continuously reviewed to identify incidents.

4.1.9 Restricted Network Access

See ITS-02: Access, Identification and Authentication Standard section 4.5 Network Access.

4.1.10 Access Control for Transmission Mediums

Physical protections must be applied to information system distribution and transmission lines to prevent accidental or intentional damage, disruption, tampering, or eavesdropping.

4.1.11 Access Control for Output Devices

Physical access to devices that could output sensitive information or data must be limited to authorized personnel. These devices include, but aren’t limited to monitors, printers, and audio devices.

4.1.12 Alternate Work Sites and Remote work

Regardless of location, whether alternate physical sites or remote work, the University must enforce safeguarding measures for all University Data.

4.2 End User Computing Physical Security

4.2.1 Unattended Systems

Equipment taken off premises (laptops, mobile devices, and other information processing equipment) must not be left unattended in public places.

4.2.2 Unattended Sessions

In accordance with the **Access, Identification and Authentication Standard**, users must terminate sessions or activate password protected screen savers prior to leaving a laptop, desktop, or system console unattended in secure and nonsecure areas. Additionally, systems must timeout sessions or activate a screen saver after periods of inactivity and require the user to reauthenticate themselves to the system.

4.2.3 Secure Work Areas

All users must clear their desks and work areas of any high or medium risk data at the end of each business day.

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	03/12/2024
Approved by:	Bret Blackman	IT CIO	03/12/2024

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published
1.1	03/12/2024	Updated Section 4.1.9 Restricted Network Access