

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
2. Scope
3. Standard Statement

1. Purpose

The purpose of the Physical Protection Standard

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.

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	03/12/2024