

---

## Data Center Physical Access

### POLICY CONTENTS

Scope  
Policy Statement  
Reason for Policy  
Procedures  
Definitions  
Related Information  
History

### Scope

This policy applies to all university personnel and entities responsible for managing and supporting Payment Card Industry (PCI)-affected systems as well as those who are responsible for the acceptance and processing of payment card transactions.

This policy affects those PCI-identified systems along with campus wide implemented systems. Those systems that are not centrally managed are to use this policy as best practices for information systems security within their respective information systems environments.

### Policy Statement

All data centers will abide by the following physical security requirements.

- Video surveillance will be installed to monitor access into and out of data centers.
- Access to data centers will be accomplished with the use of electronic badge systems.
- Physical access to data centers is limited to Information Services (IS) personnel, designated approved employees, or contractors whose job function or responsibilities require such physical access.
- University of Nebraska Omaha (UNO) staff IDs must be presented for access to data centers.
- Visitors accessing data centers will be accompanied by authorized personnel and all access will be logged via the Visitor Access Log.
  - # A Visitor Access Log will be stored at each data center.

- # Each visitor and accompanying authorized personnel must sign in and out of the data center.
- # The log will be kept for a period of at least three (3) months.
- # Physical access requires the approval of the department head responsible for the data center.
- # Physical access privileges to data centers will be audited on an annual basis.

## Reason for Policy

In accordance with Payment Card Industry Data Security Standards (PCI-DSS) requirements, UNO has established a formal policy supporting procedures regarding access to IS data centers, including payment card processing and/or storage facilities.

## Procedures

The procedures, which ensure that this policy adheres to the requirements as set forth for PCI-DSS compliance, require observance of the aforementioned policies.

## Definitions

**Data Center:** Any facility that processes, stores, or transmits cardholder data, including departments that process cardholder data and store paper copies of remittance advices.

**Cardholder Data:** Cardholder data is any personally identifiable information associated with a user of a credit/debit card. Primary account number (PAN), name, expiry date, and card verification value (CVV) are included in this definition.

## Related Information

[UNO Systems Access Control Policy](#)

---

This policy covers the following sections of PCI-DSS 3.2:

- 9.2 Develop procedures to easily distinguish between onsite personnel and visitors.

## History

This policy is an update to the Physical Access Policy that was previously updated in 2015.

---

The University of Nebraska does not discriminate based on race, color, ethnicity, national origin, sex, pregnancy, sexual orientation, gender identity, religion, disability, age, genetic information, veteran status, marital status, and/or political affiliation in its programs, activities, or employment.

