UN Data Center Security PCI Access Policy

POLICY CONTENTS

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.

University business units are responsible for following the information security policy development and implementation process established by this policy, communicating their information security policies effectively, reviewing and updating their information security policies regularly, and monitoring their information security policies for compliance and effectiveness.

Policy Statement

Media will be secured at all times, and when no longer needed for business or legal reasons, will be destroyed as defined in the Cardholder Data Access Procedures.

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 and to physical copies of cardholder data will be restricted. Where possible, access will be accomplished with the use of electronic badge systems. When not possible, access will be manually logged through a Visitor Access Log as defined in the Data Center Access Procedures. When physical copies of cardholder data are moved between physical locations, the delivery method will be tracked as defined in the Cardholder Data Access Procedures.
- Physical access to data centers is limited to Information Technology Services (ITS) personnel, designated approved employees, or contractors whose job function or responsibilities require such physical access.
- University of Nebraska staff IDs must be presented for access to data centers.
- University procedures for removing access for employees no longer employed by the university, or for employees transferred away from a data center access role, will be followed.
- Visitors accessing data centers will be accompanied by authorized personnel and all access will be logged via the Visitor Access Log as defined in the Data Center Access Procedures.
- Visitors needing access to the network will be allowed by authorized personnel to only authorized systems, and their access will be monitored.
- There will be no network jacks available to visitors in the data center unless previously authorized, and access will only be allowed during the time of the visit.

Reason for Policy

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

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

Cardholder Data Access Procedures
Data Center Access Procedures

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

- 9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
- 9.2 Develop procedures to easily distinguish between onsite personnel and visitors.
- 9.3 Control physical access for onsite personnel to sensitive areas.
- 9.4 Implement procedures to identify and authorize visitors.
- 9.5 Physically secure all media.
- 9.6 Maintain strict control over the internal or external distribution of any kind of media.
- 9.7 Maintain strict control over the storage and accessibility of media.
- 9.8 Destroy media when it is no longer needed for business or legal reasons.
- 9.10 Ensure policies and procedures for restricting physical access to CHD are documented, in use, known

History

This policy is a new policy created in 2017.