UN Systems Access Control PCI Policy

Scope

This policy applies to any university employee, contractor, or third party who has access to university PCI DSS cardholder data. This policy affects systems implemented on the university network or any system that in the course of standard business operations represents the university.

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

Access Management

All computer equipment and media used in the redirection for the transmission of cardholder information to a third party provider are to be secured and physically protected according PCI DSS requirements. The controls and protection are in place to prevent damage to assets, minimize interruption to business activities, and protect confidential data.

Need to Know

Individuals having elevated access privileges (e.g. system administrators) are prohibited from accessing information they otherwise would not have a need to know, unless required to do so in the performance of specific tasks to support critical system needs. All such access must be logged and periodically reviewed. Enforcement of this standard requires sufficient resources to carefully monitor system logs.

Privilege Assignment

Formal standards and procedures cover all stages in the lifecycle of user access, from the initial registration of new users to the final termination of users who no longer require access to information systems and services. The use of roles, policies, and attributes simplifies the administration of security by permitting access privileges to be assigned to groups of users versus individual users.

Review of Administrative Rights

The privileges granted to university employees handling cardholder data will be periodically reviewed by information owners and/or custodians to ensure university employees have access only to data they have a need to know. Access control change forms and current system access control settings will be used during the review of access privileges for university employees as per the System Access Procedures.

Customary Separation

Email access is allowed through the communicated separation date, in consideration that the employee complies with all usage restrictions as communicated at the time of separation. Exception guidelines are available in System Access Procedures.

Identification and Authentication

University employees must provide valid identification and pass background checks before being granted access to PCI DSS university computing resources. The process used for employees, students, and special access can be found in the System Access Procedures.

Identification Assignment

Each user of university computing resources redirecting the transmission of cardholder data must be assigned a unique User ID for use during the authentication (login) process. Users are forbidden to share their User ID and will be held responsible for activities that take place using their user accounts. Users with a need for privileged access are to use their standard account for normal access. When privileged access is required, the activity must be logged as per Audit Logging and Review policy. Shared access accounts are not allowed to access devices transmitting cardholder data.

Dormant User Identification
User accounts utilized to access systems transmitting cardholder data must be automatically or manually reviewed every ninety (90)-days. User accounts must be disabled if they have not been used for ninety (90) days.

Password Requirements
Passwords are set upon initial account setup. Passwords utilized on systems transmitting cardholder data must meet the PCI DSS requirement 8.2. Accounts on these systems must have passwords:

- Minimum password length of seven (7) characters
- Password expiration after ninety (90) days
- Passwords contain a combination of numeric and alphanumeric characters
- Password history maintained of at least four (4) different passwords
- Minimum password age of ten (10) days (to prevent rapid changing of password back to original)
- Unsuccessful password attempts limited to five (5)
- Account lockout of thirty (30) minutes
- Help Desk and Network Administrators can override the account lockout

The Information Technology Services Help Desk personnel and/or administrators of university information system resources will assign user passwords during initial account setup and will reset passwords only when requested by account owners or the respective department security manager. Wherever systems software permits, passwords, assigned either as a new password for a new account or as a reset, must be valid only for the initial login. At that time, the system must force users to choose and set a different password for their account. All passwords stored on university information systems or within applications and databases must be encrypted using a university-approved encryption algorithm. Under no circumstances may passwords be stored or transmitted in plaintext format. This includes batch files, automatic login scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Similarly, passwords must not be written down in some readily decipherable form and left in a place where unauthorized persons may discover them.

Minimum Controls for Authentication Credentials
Systems transmitting cardholder data must not be left unattended in locations where unauthorized persons might gain access to them.

Users must lock systems that their account is logged into before they leave the system for extended periods of time as defined in the System Access Procedures. All potential security violations are to be reported as defined in the Digital Security Incident Response policy.

Session Timeouts
Systems transmitting cardholder data must be logged-off or locked prior to being left unattended for an extended period of time as defined in the System Access Procedures. Settings must require password entry to unlock the screen.

Mobile Computing Devices
Mobile Computing Devices used to take payments must follow the mobile device requirements, found at http://pci.unl.edu/mobile-device-requirements. This includes utilizing security controls managed by ITS such as personal firewall technology.

POS Swipe Devices
Devices that capture payment card data via direct physical interaction with the card will be protected from tampering and substitution. Documentation of the POS swipe devices will be kept as outlined in the Cardholder Data Access procedures. Personnel utilizing POS swipe devices will be trained annually on methods of recognizing equipment tampering.

Network Security

Access to both internal and external networked services must be controlled. This is necessary to ensure users who have access to networks and network services do not compromise the security of these network services by ensuring:

- Appropriate interfaces between the university's network and other external networks
- Appropriate authentication mechanisms for users and equipment
- Control of user access to information services

University merchants are not allowed to utilize wireless networks to transmit cardholder data. If mobile technology is necessary, merchants will work with Information Technology Services to utilize approved mobile systems utilizing an approved cellular network.

A current network diagram that identifies all connections between the cardholder data environment and other networks must be developed and maintained. In addition, a current diagram showing all cardholder data flows across systems and networks shall be updated at least annually, or when modifications are made.

Management of network components will be performed by the university's ITS department, where systems redirecting the transmission of cardholder data exists. System components transmitting cardholder data will be placed in a segregated network zone, segregated from the DMZ and other untrusted networks.

Router configuration files will be secured and synchronized. Private IP addresses and routing information will not be disclosed to unauthorized parties.

Scans of the wireless network will be conducted to ensure there are no rogue access points present on the network where systems transmitting cardholder data exists.

Network Trust

University employees must not establish connections with external networks (including Internet Service Providers) unless these connections have been approved by the Information Security Office. All inbound session connections to university computers from external networks (e.g. the Internet) must be protected with an approved password access control system. The university network perimeter must be defined. Information security requirements have been established for network connections to entities existing outside the network perimeter.

Intrusion detection and/or intrusion prevention applications or appliances will be utilized to detect and/or prevent intrusions into the university network. The perimeter of the CDE and critical points on the network will be monitored.

Internal and external penetration testing will be performed on the CDE perimeter and critical systems by qualified personnel. The testing will occur at least annually and after any significant infrastructure or application upgrade, as defined in the PCI DSS requirements.

Firewalls

A firewall must be configured at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone where cardholder data transmission is redirected to a third party processor. Inbound and outbound traffic will be restricted to that which is necessary for those systems, and specifically deny all other traffic. Direct public access between the Internet and any system component in the cardholder data environment will be prohibited.

Network devices performing firewall functionality must be configured to support a least-privilege approach to security, allowing only specific systems, services, and protocols to communicate through the network perimeter. All default operating system and firewall application security features must be reviewed and configured to meet this requirement. Logical and physical access to these systems must be limited to those personnel with specific training and authorization to manage the device. Changes to firewall settings must follow change management policies and procedures.

See the System Access Procedures for further details regarding firewalls.

Remote Access

Only virtual private network (VPN) technologies approved by the Information Security Office are permitted to be connected to the university network environment for remote access to systems in the cardholder data environment. All proposed changes or additions to any VPN configuration(s) must undergo a risk evaluation and have written approval from the CISO or their delegated representative.

Remote access to technology in CDE must be accessed with the use of two factor authentication methods. Use of two factor must be assigned to an individual account and not shared among multiple accounts. In addition, physical or logical controls are utilized to ensure only the intended account can use the two factor as outlined in the System Access procedures.

Reason for Policy

Physical and logical access to systems transmitting cardholder data in the possession of, or under the control of the university must be restricted to authorized individuals. This policy outlines the requirements for logical access controls with the intent of reducing the risk of unauthorized access to university information assets. This also outlines the procedures for removal of access with regard to employee separations. Detailed separation guidelines and checklists are identified in the System Access Procedures.

Definitions

Cardholder Data/CDE: Cardholder data is any personally identifiable information associated with a user of a credit/debit. Primary account number (PAN), name, expiry date, and card verification value 2 (CVV2) are included in this definition.

Minimum Necessary/Least Privilege: The concept that all users at all times are to perform their job duties with as few privileges as possible.

Separation Date: Date at which employee separation becomes official.

Collaboration Tools: The tools provided for communication and collaboration. These include, but are not limited to email, instant messaging, phone, and voicemail.

Account: Typical access ID used for the access of applications and systems.

Privilege: Access to university resources.

Authentication Credentials: Identifying information that when used in conjunction with a password or passcode allows access to a protected resource.

Virtual Private Network (VPN): Protects data transfers between two or more networked devices so as to keep the transferred data private from other devices on one or more intervening local or wide area networks.

University Administrative Designee: Senior Vice Chancellor, Vice Chancellor, or the Assistant to the Senior Vice Chancellor for Human Resources and Academic Affairs.

Related Information

Additional Contacts

- **Director of Human Resources (HR):** Responsible for the notification and facilitation of employee separations.
- **Administrative Designee:** Responsible for enforcement of this policy relative to faculty governance.
- **Chief Information Officer (CIO):** Responsible for enforcing technology requirements outlined in this policy.
- **Chief Information Security Officer {CISO):** Responsible for the enforcement of this policy as well as consulted on the determination of risk in conjunction with the Director of HR on matters of employee separation.

NU Executive Memorandum 16
NU Executive Memorandum 26
State of Nebraska Consumer Notification of Data Security Breach Act of 2006
Digital Security Incident Response Policy

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

- 1.1 Establish and implement firewall and router configuration standards
- 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment

- 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment
- 1.4 Install firewall software or equivalent on any portable computing devices
- 1.5 Ensure policies and procedures for managing firewalls are documented, in use, and known
- 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access
- 7.2 Establish an access control system for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed
- 7.3 Ensure policies and procedures for restricting access to CHD are documented, in use, and known
- 8.1 Define and implement policies and procedures to ensure proper user identification management
- 8.2 Ensure proper user-authentication management for non-consumer users and administrators on all system components
- 8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication
- 8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods
- 8.6 Two factor procedures
- 9.9 Protect devices that capture payment card data via direct physical interaction with the card
- 10.1 Implement audit trails to link all access to system components to each individual user
- 10.9 Ensure policies and procedures for monitoring network and CHD are documented, in use, and known
- 11.1 Implement processes to test for the presence of wireless access points on a quarterly basis
- 11.3 Penetration testing
- 11.4 IDS or IPS techniques
- 11.6 Ensure policies and procedures for security monitoring are documented, in use and known
- 12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
- 12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources

History

This policy is a new policy created in 2017.