Nebraska Brand Committee

Information Security Policy

Payment Card Industry Data Security Standard Compliant

Template provided by Nebraska State Treasury Department

About This Document

This document contains the Nebraska State agencies policies as they relate to information security. Throughout this document are references to supporting documents which contain more detailed information and guidance on specific standards and procedures. This document is for internal use only and is not to be distributed.

Table 1 - Revision History

Version	Date	Author	Description of Change
1.0	December 1, 2020	Rebekah Vineyard	Document created
			Template provided by Nebraska State Treasury Department

Contents

Build and Maintain a Secure Network and Systems

Section 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between State of Nebraska's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within the State of Nebraska's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment.

Section 1.1: Establishment and Implementation of Firewall and Router Configuration Standards

- Nebraska Information Technology Commission's (NITC) 7-201 Network Edge Device Standard for Entities Choosing to Connect to Network Nebraska[1] document details our policies and procedures for implementation and establishment of firewall and router configuration standards and must be followed.
- The Firewall and Router Configurations must restrict connections between untrusted networks and system components in the Cardholder Data Environment
- The Firewall and Router Configurations must prohibit direct public access between the Internet and any system component in the Cardholder Data Environment as stated in NITC 7-101 and NITC 8-101, 4.8.1.3.

[1] See *NITC Standards & Guidelines 7-201*

Section 2: Do Not Use Vendor Supplied Defaults for System Password and other Security Parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Nebraska State agencies will always change the vendor-supplied defaults for system passwords and other security parameters before systems are installed in the secure network environment (cardholder data network).

Section 2.1: Change Vendor Supplied Defaults Prior to Installation

- The vendor-supplied defaults must be changed on all system components prior to installation in the cardholder data network. This includes all passwords and simple network management protocol (SNMP) community strings. (Addresses Payment Card Industry (PCI) DSS Requirement 2.1.a, 2.2.d)
- Any unnecessary default accounts must be removed or disabled prior to installation in the cardholder data network. (Addresses PCI DSS Requirement 2.1.b)
- For wireless environments connected to the cardholder data network or transmitting cardholder data:
  - All default settings for wireless equipment must be changed prior to touching cardholder data. (Addresses PCI DSS Requirement 2.1.1.a-e)
  - Encryption keys or passphrases must be changed anytime anyone with knowledge of the keys leaves the company or changes to a position that does not require knowledge of the keys or passphrases. (Addresses PCI DSS Requirement 2.1.1.a)
  - All wireless device firmware configurations must be updated to support strong encryption for both network authentication and data transmission. (Addresses PCI DSS Requirement 2.1.1.d)

Section 2.2: System Configuration and Hardening Standards

To establish consistency with SANS, ISO, NIST, CIS, or similar security industry standards and address PCI configuration requirements (e.g., password requirements, log settings, File Integrity Monitoring, anti-virus software, etc.), state agencies require documented standards to be developed that address all system components and address all known security vulnerabilities for systems used in the cardholder data network. The NITC Standards & Guidelines 8-103[2] document, details our policies and procedures for configuration and hardening of the system.

- These standards must be updated as new vulnerabilities are identified (See Section 6.1) and be applied when new systems used in the card network are configured and before systems are placed into production.

[2] See the *NITC Standards & Guidelines 8-103* document.

Section 2.3: Use Secure Protocols for Non-Console Access

- Strong cryptography must be used for any non-console or web-based management interface used for administration of systems or system components. (Use technologies such as SSH, VPN, or the latest secure versions of TLS (1.1 or higher) for web-based management and other non-console administrative access.) (Addresses PCI DSS Requirement 2.3)

Section 2.4: System Inventory

- Each state agency maintains an inventory of system components relevant to the scope of PCI DSS. (This should include a system inventory for systems within the Cardholder Data Environment, critical software, any third party payment solutions being used (if applicable), service providers with which cardholder data is being shared (if applicable). See Appendix E.

Section 2.6: Shared Hosting Providers

- Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A of the PCI Standards Document: Additional PCI DSS Requirements for Shared Hosting Providers.* (Addresses PCI DSS Requirement 2.6)

Section 3: Protect Stored Cardholder Data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. Credit card data has many sensitive components, including the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN), etc.

The following policies address the treatment of credit card data.

Section 3.2: Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?

- POS systems are to be updated with the most current version of software that is provided by the manufacturer which does not store the full contents of any track from the magnetic stripe (located on the back of the card, contained in a chip, or elsewhere). Document all software upgrades on the Processing Equipment Maintenance Form.
- Do not store the card verification code or value (three-digit or four-digit number printed on the bank of the payment card) used to verify card-not-present transactions.
- Do not store the personal identification number (PIN) or the encrypted PIN block.

Section 3.3: Mask Credit Card Numbers in Displays Wherever Possible

- Credit card PAN Data will be masked or truncated when displaying card numbers (Standards say the first six and last four digits are the maximum number of digits to be displayed) on any media. However, we recommend that only the last four digits be printed on any receipt or report. Only personnel with a legitimate business need and proper written approval can see more than the last four digits of the PAN[3]. (Addresses PCI DSS Requirement 3.3)

[3] See Appendix A (*Authorized Users List)*

Section 4: Encrypt Transmission of Cardholder Data across Open, Public Networks

Cardholder data must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

Section 4.1: Transmission of Card Data over Public Networks (If applicable)

- Strong cryptography and security protocols (e.g., TLS 1.1 or higher, IPSEC, SSH greater than v1.0) must be used whenever cardholder data is transmitted or received over open, public networks. The following controls must be part of the State of Nebraska/NITC data transmission policies: (Addresses PCI DSS Requirement 4.1.a)
    - Only trusted keys and certificates will be accepted. (Addresses PCI DSS Requirement 4.1.b)
    - The data transmission protocol only supports secure versions or configurations and does not support insecure versions or configuration. (e.g., use the latest secure TLS and SSH versions only). (Addresses PCI DSS Requirement 4.1.c)
    - The encryption strength is appropriate for the encryption methodology in use. (Addresses PCI DSS Requirement 4.1.d)
    - For TLS implementations, TLS must be enabled whenever cardholder data is transmitted or received. (Addresses PCI DSS Requirement 4.1.e)
    - If SSL or early TLS is used on a POS POI terminal, a migration plan must be created and implemented, documentation must be created detailing how it was verified that the terminal is not susceptible to any known exploits for SSL or early versions of TLS. Documentation must include evidence (vendor documentation, system/network configuration details, etc). (Addresses PCI DSS Requirement 4.1.f)
    - If SSL or early TLS is used anywhere but a POS POI terminal, a risk mitigation and migration plan must be created, which includes the following: (Addresses PCI DSS Requirement 4.1.g)
        - Description of how it is used, including what data is being transmitted, the types and number of systems that use and/or support SSL or early TLS and the type of environment.
        - The risk assessment results, including the risk reduction controls that are in place.
        - A process of how new vulnerabilities associated with SSL and early TLS are monitored.
        - A description of change control processes that are in place to ensure no new environments are created which utilize SSL and/or early TLS.
        - An overview of the migration project plan that includes a migration completion date no later than June 30th, 2018.

- If wireless networks transmitting cardholder data or connected to the cardholder data environment are in use, a documented standard must be created which ensures the use of strong encryption and industry best practices. (Addresses PCI DSS Requirement 4.1.1)

Section 4.2: Transmission of Card Data via End User Messaging Technologies

- It is prohibited to transmit unencrypted cardholder data via end-user messaging technologies (e.g., e-mail, instant messaging, etc.). (Addresses PCI DSS Requirement 4.2)

Section 5: Protect All Systems against Malware and Regularly Update Anti-Virus Software or Programs

Malicious software, commonly referred to as malware, enters a sensitive network segment during many business approved activities, including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

Section 5.1: Deploy anti-virus software to protect systems

- Anti-virus software must be deployed on all systems in the card network that are commonly affected by malicious software. This includes personal computers, servers, etc. that are attached to the cardholder network segment. (Addresses PCI DSS Requirement 5.1)
- Anti-virus programs must be capable of detecting, removing, and protecting against all known types of malicious software (adware, spyware, etc.). (Addresses PCI DSS Requirement 5.1.1)
- For systems considered not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue not to require anti-virus software. (Addresses PCI DSS Requirement 5.1.2)

Section 5.2: Ensure that all anti-virus mechanisms are maintained

- All anti-virus software and its associated definition files must be kept up-to-date at all times. (Addresses PCI DSS Requirement 5.2.a)
- All anti-virus software must be actively running, configured to perform automatic updates, and set to run periodic scans. (Addresses PCI DSS Requirement 5.2.b & c)
- Anti-virus software must be capable of generating audit logs and audit logs must be retained for one year. (Addresses PCI DSS Requirement 5.2.d)

Section 5.3: Ensure that all anti-virus mechanisms are actively running

- All anti-virus software installations and configurations must be actively running at all times. (Addresses PCI DSS Requirement 5.3.a)
- Anti-virus configurations do not allow users to disable or alter the software unless specifically authorized by management on a case-by-case basis for a limited time. (Addresses PCI DSS Requirement 5.3.b & c)

Section 6: Develop and Maintain Secure Systems and Applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations.

Section 6.1: Vulnerability risk ranking process

- System administrators are to subscribe to outside sources for security vulnerability information and system configuration standards are to be reviewed and updated as new vulnerability information might dictate. Outside sources might include SecurityFocus, A/V companies, SANS, CIS, Secunia, Microsoft, etc. (Addresses PCI DSS Requirement 6.1)

When any vulnerability (or potential vulnerability) is found using NITC Standards & Guidelines 8-101[4], it must be evaluated and assigned a ranking based on the risk level. At a minimum, the highest risk vulnerabilities should be assigned a "High" risk ranking. (Addresses PCI DSS Requirement 6.1)

Section 6.2: Regularly update systems and software

Patch Management Process

- All system components and software must have the latest vendor-supplied security patches installed. (Addresses PCI DSS Requirement 6.2.a)
- All critical system and software patches must be installed within 30 days of vendor release. (Addresses PCI DSS Requirement 6.2.b)
- A server's OS version, all packages and installed applications versions and patch levels are inventoried centrally. Each system's list of software is compared to a master list of minimum required versions in order to ensure there are no security vulnerabilities present. The master list is maintained by automatically retrieving a list of latest patch levels, as well as by monitoring for security alerts in mailing lists and security web sites for all installed applications.

As industry best practices for vulnerability management are updated, NITC will modify vulnerability management practices to stay in sync with the most recent developments. Procedures related to PCI DSS 6.5.1-6.5.10 will be modified to match industry best practices. (Addresses PCI DSS Requirement 6.5)

[4] See the *NITC Standards & Guidelines 8-101* document.

Section 6.6: Protect Exposed Web Applications

For public-facing web applications, ensure that either one of the following is in place:

- Public-facing web applications must be reviewed (using either manual or automated vulnerability security assessment tools or methods) as follows: (Addresses PCI DSS Requirement 6.6)
  - At least annually.
  - After any changes.
  - By an organization that specializes in application security (can be a separate internal company team, independent of the development team that has been trained appropriately).
  - All vulnerabilities in PCI DSS Requirement 6.5 are included.
  - All vulnerabilities must be corrected.
  - The application is re-evaluated after corrections have been made.
- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, which continually checks all traffic. The solution must meet the following requirements: (Addresses PCI DSS Requirement 6.6)
  - Is situated in front of public-facing web applications.
  - Is actively running and updated as applicable.
  - Is generating audit logs.
  - Is configured to either block web-based attacks, or generate an alert.

Section 7: Restrict Access to Cardholder Data by Business Need to Know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to the least amount of data and privileges needed to perform a job.

Section 7.1: Limit Access to Cardholder Data and Systems in Cardholder Data Environment

- Access to cardholder data and system components must be restricted to only those individuals whose job requires such access. (Addresses PCI DSS Requirement 7.1)
- Define access needs for each role, including: (Addresses PCI DSS Requirement 7.1.1)
    - System components and data resources that each role needs to access for their job function.
    - Level of privilege required for accessing resources (for example, user, administrator, etc.).
- Restrict access to privileged user IDs to the least privileges necessary to perform job responsibilities and assigned to only those roles that specifically require the privileged access. (Addresses PCI DSS Requirement 7.1.2)
- Access assigned to individual personnel is based on their job classification and function. (Addresses PCI DSS Requirement 7.1.3)
- Require an authorization form specifying all required access privileges, which must be generated and signed by management approving the access. (Addresses PCI DSS Requirement 7.1.4)

Section 7.2: Access Control Systems

- Access control systems for systems components must restrict access based on a user’s need to know. (Addresses PCI DSS Requirement 7.2)
- Access controls are required on all system components of the cardholder data environment and must be implemented via an automated access control system. (Addresses PCI DSS Requirements 7.2.1)
- Access controls are required to enforce privileges assigned to individuals based on job classification and function. (Addresses PCI DSS Requirements 7.2.2)
- Access control systems must also be set to a default “deny-all” setting. (Addresses PCI DSS Requirements 7.2.3)

Section 8: Identify and Authenticate Access to System Components

Assigning a unique identification (ID) to each person with access to critical systems or software ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Note that these requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance). These requirements do not apply to accounts used by consumers (e.g., cardholders).

Section 8.1: Require Unique User IDs

- Unique IDs will be used for all users that access system components or cardholder data. (Addresses PCI DSS Requirement 8.1.1)
- Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. (Addresses PCI DSS Requirement 8.1.2)
- Immediately revoke access for any terminated users. (Addresses PCI DSS Requirement 8.1.3)
- Remove/disable inactive user accounts at least every 90 days. (Addresses PCI DSS Requirement 8.1.4)
- Manage IDs used by all third parties with remote access to access, support, or maintain system components via remote access, ensuring that they are only enabled for the time period needed, disabled when not in use, and they are monitored by agency employees during use. (Addresses PCI DSS Requirement 8.1.5)
- Limit repeated access attempts by locking out the user ID after not more than six attempts. (Addresses PCI DSS Requirement 8.1.6)
- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (Addresses PCI DSS Requirement 8.1.7)
- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. (Addresses PCI DSS Requirement 8.1.8)

Section 8.2: User Authentication Methods

- In addition to assigning a unique user ID, access to systems in the card network requires the use of at least one of the following: (Addresses PCI DSS Requirement 8.2)
  - Something you know, such as a password or passphrase
  - Something you have, such as a token device or smart card
  - Something you are, such as a biometric
- Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. (Addresses PCI DSS Requirement 8.2.1)
- Verify user identity before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys.) (Addresses PCI DSS Requirement 8.2.2)
- Passwords or phrases must meet the following: (Addresses PCI DSS Requirement 8.2.3)
  - Require a minimum length of at least seven characters
  - Contain both numeric and alphabetic characters

- ❖ Change user passwords/passphrases at least every 90 days. (Addresses PCI DSS Requirement 8.2.4)
- ❖ Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/phrases they have used. (Addresses PCI DSS Requirement 8.2.5)
- ❖ Set all first time use and reset passwords to a unique value for each user and require immediate change after first use. (Addresses PCI DSS Requirement 8.2.6)

Section 8.3: Multi-factor Authentication

- ❖ Incorporate multi-factor authentication for remote network access originating from outside the network by personnel, including users and administrators and all third parties, including vendor access for support or maintenance. (Addresses PCI DSS Requirement 8.3)
- ❖ Incorporate multi-factor authentication for all console and non-console access into the CDE for personnel with administrative access. (Addresses PCI DSS Requirement 8.3.1)

Section 8.4: Password Policy

- ❖ Document and communicate authentication procedures and policies to all users including: (Addresses PCI DSS Requirement 8.4)
  - ➢ Guidelines for selecting strong authentication credentials.
    - ▪ All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least every 90 days.
    - ▪ All production system-level passwords must be part of the agency administered password log.
    - ▪ All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
    - ▪ Passwords must change upon initial logon, system permitting, by the user and subsequently changed at least every 90 days.
    - ▪ All user-level and system-level passwords must conform to the guidelines described below.
  - ➢ Guidelines
    - ▪ All users at a state agency should be aware of how to select strong passwords. Strong passwords have the following characteristics:
      - Contain at least three of the five following character classes:
        - Lower case characters
        - Upper case characters
        - Numbers
        - Punctuation
        - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
        - Contain at least ten alphanumeric characters.
      - Weak passwords have the following characteristics:
        - The password contains less than ten characters
        - The password is a word found in a dictionary (English or foreign)
        - The password is a common usage word such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words “State of Nebraska”, "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

➢ Password Protection Standards
- Always use different passwords for agency accounts from other non-agency access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various agency access needs whenever possible.
- Passwords must not repeat any of the four most recently used passwords.
- Do not share agency passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential agency information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the IT Administrator. If an account or password compromise is suspected, report the incident to the IT Administrator

➢ Instructions to change passwords if there is any suspicion the password could be compromised.
- Validating requests to change passwords should include face-to-face verification, or having the team member validate their identity by answering their authentication questions and answers (minimum six questions and three correct answers). Once the team member is positively identified, a new password will be automatically generated (using a valid password generation program) to provide to the team member.

Section 8.5: Group or Shared Passwords

❖ Do not use group, shared, or generic password or other authentication methods as follows: (Addresses PCI DSS Requirement 8.5.)
- ➢ Generic user IDs are disabled or removed.
- ➢ Shared user IDs do not exist for system administration and other critical functions.
- ➢ Shared and generic user IDs are not used to administer any system components.

Section 8.6: Other Authentication Mechanisms

- Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: (Addresses PCI DSS Requirement 8.6)
  - Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
  - Physical or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

Section 9: Restrict Physical Access to Cardholder Data

Any physical access to data or systems that house cardholder data provide the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

- NITC Standards & Guidelines 8-101[5] document details our policies and procedures for restricting physical access to cardholder data and must be followed at all times. (Addresses PCI DSS Requirements 9.1 – 9.10)
- PCI paper shall not be generated.

Section 9.5: Are all media physically secured (Including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?

- All media shall remain within the locked, secured, office premises, until such time, as required for the media, that it is destroyed. If any paper media is created by the card swipe machines, this media will be shredded.

Section 9.6: Is strict control maintained over the internal or external distribution of any kind of media?

- Locate all paper documents (including receipts, notes, reports and faxes) and all electronic storage data (if any type) which contain your customers' full credit/debit card numbers and mark the container as "Confidential".
- Media will not be transported or delivered outside the secured perimeter of the office.
- Only authorized individuals will handle media within the confines of the office secured space.

Section 9.7: Is strict control maintained over the storage and accessibility of media?

- No material will be removed from the secure area.

Section 9.8: Is all media destroyed when it is no longer needed for business or legal reasons?

- All hardcopy (paper) media will be destroyed by a crosscut shredder immediately.

Section 9.9: Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows?

- A list of POS devices shall be maintained along with a list of authorized users. This list will include the make and model of device, the location of the device, and the device serial number. The list will be updated when devices are added, relocated, or decommissioned.

---

[5] See the *NBC Standards & Guidelines 8-101* document.

- ❖ Devices will be periodically inspected to look for tampering or substitution by checking the serial number and other device characteristics. Personnel will be trained annually on how to inspect POS devices for tampering.
- ❖ Personnel will be trained to be aware of suspicious behavior and to report tampering or substitution of devices. Personnel are to verify the identity of repair or maintenance personnel. Devices will not be installed, replaces, or returned without verification. Personnel will report any indication of suspicious behavior or of device tampering to their manager.

Section 10: Track and Monitor All Access to Network Resources and Cardholder Data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

Section 10.1: Enable Audit Trails to Link Access to System Components

- Enable audit trails on all system components within the cardholder data network to link all access to system components to each individual user. (e.g., server event logs, web server logs, firewall logs, payment application logs, etc.). (Addresses PCI DSS Requirement 10.1)

Section 10.2: Generation of Automated Audit Trails

- Implement automated audit trails for all system components to capture the following events: (Addresses PCI DSS Requirement 10.2)
  - All individual access to cardholder data.
  - All actions taken by any individual with root or administrative privileges.
  - All access to audit trails.
  - Invalid logical access attempts.
  - Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.
  - Initialization, stopping, or pausing the audit logs.
  - Creation and deletion of system level objects.

Section 10.3: Audit Trail Entries

- Record at least the following audit trail entries for all system components for each event: (Addresses PCI DSS Requirement 10.3)
  - User Identification
  - Type of event
  - Date and Time
  - Origination of event
  - Identity or name of affected data, system component, or resource

Section 10.4: Network and System Time Sync

- The Nebraska State Treasurer's Office Network Time Protocol (NTP) Configuration Procedures[6] document details the process for obtaining and distributing a time signal (system time) to all system components within the cardholder data network. (Addresses PCI DSS Requirement 10.4)
- Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time: (Addresses PCI DSS Requirement 10.4)
    - A central timeserver is designated, and if there are multiple servers, the servers are configured to peer with each other to keep accurate time. (Addresses PCI DSS Requirement 10.4.1)
    - All other components in the CDE receive time only from the designated central timeserver. (Addresses PCI DSS Requirement 10.4.1)
    - Critical systems have the correct and consistent time. (Addresses PCI DSS Requirement 10.4.1)
    - Time data is protected through access to time data restricted to only personnel with a business need. (Addresses PCI DSS Requirement 10.4.2)
    - All time settings on critical systems are logged, monitored, and reviewed. (Addresses PCI DSS Requirement 10.4.2)
    - Time settings are received from industry-accepted sources. (Addresses PCI DSS Requirement 10.4.3)

Section 10.5: Audit Trail Security

- Secure audit trails so they cannot be altered as follows: (Addresses PCI DSS Requirement 10.5)
    - Limit viewing of audit trails to those with a job-related need. (Addresses PCI DSS Requirement 10.5.1)
    - Protect audit trail files from unauthorized modifications. (Addresses PCI DSS Requirement 10.5.2)
    - Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Addresses PCI DSS Requirement 10.5.3)
    - Write logs for external-facing technologies onto a secure, centralized log server or media device. (Addresses PCI DSS Requirement 10.5.4)
    - Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. (Addresses PCI DSS Requirement 10.5.5)

Section 10.6: Log Review

- Review logs and security events for all system components to identify anomalies or suspicious activity. (Addresses PCI DSS Requirement 10.6)
- Review the following at least daily:
    - All security events.
    - Logs of all system components that store, process, or transmit cardholder data, or that could affect the security of cardholder data.
    - Logs of all critical system components.

---

[6] See the *NBC's Configuration Procedures* document.

- Logs of all servers and system components that perform security functions (for example, firewalls, IDS/IPS, authentication servers, e-commerce redirection servers, etc.).

- Review logs of all other system components periodically, based on the organization's policies and risk management strategy, as determined by NITC's Annual Risk Assessment[7]. Until NITC Annual Risk Assessment document is complete, the Agency Information Security Officer or designated employee shall review logs from servers and card applications. (Addresses PCI DSS Requirement 10.6.2)
- Immediately follow up on exceptions and anomalies identified during the review process. (Addresses PCI DSS Requirement 10.6.3)

Section 10.7: Audit Trail History

- Retain audit trail history for at least one year with a minimum of three months immediately available for analysis (e.g., online, archived, or restorable from backup). (Addresses PCI DSS Requirement 10.7)

[7] See the *NBC's Annual Risk Assessment is being addressed*.

Section 11: Regularly Test Security Systems and Processes

System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment. Detailed testing procedures[8] should be developed and documented to meet the following policies.

Section 11.1: Rogue Wireless Network Detection

- NITC Standards and Guidelines 7-301[9] describes the documented process that will be used at least quarterly to detect unauthorized wireless networks/devices within the card-processing environment. (Addresses PCI DSS Requirement 11.1 and 11.1.2)
- The defined methodology will address the detection and identification of multiple types of wireless devices such as WLAN cards inserted into system components, portable wireless devices connected to system components, and wireless devices connected to a network port or network device. (Addresses PCI DSS Requirement 11.1)
- Any automated monitoring solution must generate alerts if rogue devices are detected.
- Process documentation must define a response procedure if rogue devices are found.
- Each agency will maintain an inventory of all authorized wireless access points including a documented business justification. (Addresses PCI DSS Requirement 11.1.1)
- The agency will define incident response procedures (see PCI DSS Requirement 12.10) in the event an unauthorized wireless access point is detected (Addresses PCI DSS Requirement 11.1.2)

Section 11.2: Vulnerability Scans

- Internal vulnerability scans must: (Addresses PCI DSS Requirement 11.2.1.a-c)
  - Be performed by a qualified internal resource with organizational independence or a qualified third party.
  - Have a process to include a rescan until all “high risk” vulnerabilities must be addressed in accordance with the entity’s vulnerability ranking (as defined in Requirement 6.1) and verified by rescans.
- External vulnerability scans must (Addresses PCI DSS Requirement 11.2.2.a-c)
  - Contain no vulnerabilities that are scored 4.0 or higher by the CVSS.
  - Run on all external IP addresses that could be used to gain access to the cardholder data environment. (Addresses PCI DSS Requirement 11.2)

- The agency must ensure that results of each quarter's internal and external vulnerability assessments are to be documented and retained for review. (Addresses PCI DSS Requirement 11.2.3) State OCIO can assist upon request.

Section 11.3: Penetration Testing

- Implement a methodology for penetration testing that includes the following: (Addresses PCI DSS Requirement 11.3)
  - Is based on industry-accepted penetration testing approaches. (for example, NIST SP 800-115)
  - Includes coverage for the entire CDE perimeter and critical systems.
  - Includes testing from both inside and outside the network.
  - Includes testing to validate all segmentation and scope reducing controls.
  - Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.
  - Defines network-layer penetration tests to include components that support network functions as well as operating systems.
  - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.
  - Specifies retention of penetration testing results and remediation activity results for at least one year.
- Internal and external penetration tests are to be performed as per the defined methodology, at least annually and after any significant infrastructure or application upgrade or modification (e.g., an operating system upgrade, a sub-network added to the environment, or a web server added to the environment, etc.). (Addresses PCI DSS Requirement 11.3.1 and 11.3.2)
- Penetration testing is to be performed by a qualified internal resource or third party. If an internal resource is used, the personnel conducting the test must be independent from personnel that work within the cardholder environment. (PCI DSS Requirement 11.3)
- Exploitable vulnerabilities found during testing are corrected and testing is repeated to confirm the correction. (Addresses PCI DSS Requirement 11.3.3)
- If segmentation is used to isolate the CDE from other networks, perform penetration tests (performed by a qualified internal resource or qualified external third party) at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. (Addresses PCI DSS Requirement 11.3.4)
- If the entity is a service provider: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. This requirement is a best practice until January 31, 2018, after which it becomes a requirement. (Addresses PCI DSS Requirement 11.3.4.1)

Section 11.4: Intrusion Detection/Prevention

- All traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder environment must be monitored by the use of an Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS). (Addresses PCI DSS Requirement 11.4.a)

- ❖ The IDS/IPS system(s) must be configured to alert personnel of suspected compromises. (Addresses PCI DSS Requirement 11.4.b)
- ❖ All IDS/IPS system(s) must be kept up to date with the latest available attack signatures. (Addresses PCI DSS Requirement 11.4.c)

Section 11.5: Change Detection

- ❖ Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. (Addresses PCI DSS Requirement 11.5)

Section 12: Maintain a Security Policy that Addresses Information Security for All Personnel

A strong security policy sets the security tone for the State of Nebraska and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. "Employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the State of Nebraska's site.

Section 12.1: Publish, Distribute, and Update the Information Security Policy

- The Nebraska Brand Committee requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (Addresses PCI DSS Requirement 12.1)
- The Nebraska Brand Committee information security policy must be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. (Addresses PCI DSS Requirement 12.1.1)

Section 12.2: Implement a Risk-Assessment Process

- NITC defines and documents a risk assessment process in the NITC Standards & Guidelines[10] document, which: (Addresses PCI DSS Requirement 12.2)
  - Is performed annually and upon significant change to the environment
  - Identifies critical assets, threats, and vulnerabilities
  - Results in a formal risk assessment.

Section 12.3: Critical Technology Usage Policies

- The State of Nebraska must develop usage policies for critical technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage), and define proper use of these technologies. (Addresses PCI DSS Requirement 12.3)
- Explicit management approval is required prior to using the technologies. (Addresses PCI DSS Requirement 12.3.1)
- Any use of the technology must be authenticated with a user ID and password or other authentication item (for example, token). (Addresses PCI DSS Requirement 12.3.2)
- A list must be maintained of all such devices in use and contain the personnel authorized to use them in the State of Nebraska agency Critical Technology Device Inventory Document Attachment F. (Addresses PCI DSS Requirement 12.3.3)
- A method to determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) accurately and readily. (Addresses PCI DSS Requirement 12.3.4)
- Acceptable uses for the technology must be defined and documented (This should include a system inventory for systems within the Cardholder Data Environment, critical software, any third party payment

[10] See the *NITC Standards & Guidelines Risk Assessment Process* document.

solutions being used (if applicable), service providers with which cardholder data is being shared (if applicable). (Addresses PCI DSS Requirement 12.3.5)

- Acceptable network locations for the technologies must be defined and documented. (Addresses PCI DSS Requirement 12.3.6)
- A list of company-approved products must be kept. (Addresses PCI DSS Requirement 12.3.7)
- Remote-access technologies in use must automatically disconnect sessions after a specific period of inactivity. (Addresses PCI DSS Requirement 12.3.8)
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners with immediate deactivation after use. (Addresses PCI DSS Requirement 12.3.9)
- Copying, moving, or storing cardholder data on local hard drives and removable electronic media when accessing such data via remote-access technologies is prohibited unless explicitly authorized for a defined business need, and the cardholder data is protected in accordance with all applicable PCI DSS requirements. (Addresses PCI DSS Requirement 12.3.10)

Section 12.4: Assign Information Security Responsibilities and Train Employees

- Nebraska Brand Committee Information Security Policy and procedures clearly define information security responsibilities for all personnel (Addresses PCI DSS Requirement 12.4)
  - If the agency is a service provider: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include overall accountability for maintaining PCI DSS compliance and defining a charter for a PCI DSS compliance program and communication to executive management. (Addresses PCI DSS Requirement 12.4.1)

Section 12.5: Assign Information Security Management

- **The overall responsibility of information security management falls under the Agency Information Security Officer or designated agency personnel.** (Addresses PCI DSS Requirement 12.5)

- The following responsibilities must be assigned: (see the Management Roles and Responsibilities form in Appendix B)
  - Establishing, documenting, and distributing the Nebraska Brand Committee's information security policies and procedures. (Addresses PCI DSS Requirement 12.5.1)
  - Responsibility to monitor, analyze, and distribute security alerts and information. (Addresses PCI DSS Requirement 12.5.2)
  - Establishing detailed documentation of security incident response and escalation procedures and formally assign the responsibility of creating and distributing these procedures to a specific role, position, or team. (Addresses PCI DSS Requirement 12.5.3)
  - Administration of user accounts in the cardholder data network. (Addresses PCI DSS Requirement 12.5.4)
  - Monitoring and controlling all access to data. (Addresses PCI DSS Requirement 12.5.5)

Section 12.6: Security Awareness Program

- NTIC Standards & Guidelines 8-101 document[11] defines the processes used by the agency to ensure personnel are aware of the cardholder data security policy and procedures. (Addresses PCI DSS Requirement 12.6.a)
- Employees working in the cardholder data environment must be educated upon hire and at least annually regarding their data security responsibilities. (Addresses PCI DSS Requirement 12.6.b)
- Security awareness training programs must employ the use of multiple methods of communicating awareness and educating employees (e.g., posters, letters, memos, web-based training, meetings, promotions, etc.). (Addresses PCI DSS Requirement 12.6.1.a)
- Employees must acknowledge in writing, at least annually, that they have read and understood the Nebraska Brand Committee Security Policies and Procedures. (Addresses PCI DSS Requirement 12.6.2)

Section 12.7: Background Checks

- Background checks are to be conducted, within the constraints of local laws, on employees, prior to hire, who will have access to cardholder data or the cardholder data environment. (Addresses PCI DSS Requirement 12.7) State of Nebraska agencies should at least do driver records, county and district court records, and a State Patrol check.

Section 12.8: Policies for Sharing Data with Service Providers

- In order to conform to industry best practices, it is required that due diligence be performed before engaging with new service providers and is monitored for current service providers that store, process, or transmit cardholder data on behalf of the state agency. Service providers, which could affect the security of sensitive cardholder data, are also in-scope of this policy. The Nebraska State Treasurer's Office Full-Service Provider Compliance Validation Procedures[12] document describes the process of validating service provider compliance with PCI DSS Requirements. (Addresses PCI DSS Requirement 12.8)

Section 12.9: Additional Requirements for Service Providers

- Service providers must acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. (Addresses PCI DSS Requirement 12.9)

Section 12.10: Incident Response Plan Policies

- The Nebraska State Treasurer's Office Incident Response Plan[13] document (IRP) explains the course of action in the event of a breach or suspected breach.
- IRP will be reviewed and tested at least annually.

---

[11] See the *NITC Standards & Guidelines 8-101* document.

[12] See the *Nebraska State Treasurer's Office Full-Service Provider Compliance Validation Process* document.

[13] See the *Nebraska State Treasurer's Office Incident Response Plan*

- A Computer Incident Response Team (CIRT) will consist of members from the State Agency, OCIO and State Treasurer's Office.
- Team members designated are to be available on a 24/7 basis to respond to alerts.
- Team members are required to understand data breach response requirements outline by each card brand.
- Training will be provided to staff with security breach response responsibilities.
- Each Team will have the following members identified and reviewed at least annually.

CIRT Members	CIRT Role
Agency Director/Manager	Provide authority to operate and has authority to make business-related decisions based on information garnered from the other team members.
State Information Security Officer	Assess security incidents, perform containment, eradication and basic forensics. Assist information technology in recovery role.
Agency Information Security Officer	Minimize the impact to system end users. Assist the Information Security team with technical issues and recovery roles.
Chief Information Officer	Understand the root cause of the incident and any failures of compliance, which may have contributed to the incident.
Network Services Administrator	Assess any physical damage and investigate any physical theft of data. Document chain of custody for any physical evidence.
Agency Legal	Ensure that evidence collected is usable in a criminal investigation. Act as legal counsel to senior management.
Agency Human Relations Representative	Provide advice to senior management if an employee caused the incident.
Public Relations – State Treasurer's Office Staff	Work with all members of the CIRT to understand the incident. Coordinate with senior management, acquirers, card brands and law enforcement to develop a disclosure plan (if any).

Appendix A – Authorized Users List

Authorized Users List

Below is a list of users authorized to view full PAN data as required by PCI DSS Requirement 3.3 and approved by the director of the agency.

[Employee Full Name]

[Employee Full Name]

[Employee Full Name]

[Employee Full Name]

Appendix B – Management Roles and Responsibilities

Assignment of Management Roles and Responsibilities for Security

As required by policy in Section 12.5 of this security policy, the following table contains the assignment of management roles for security processes.

Table A1 - Management Security Responsibilities

Name of Role, Group, or Department	Date Assigned	Description of Responsibility
		Establish, document, and distribute security policies
		Monitor, analyze, and distribute security alerts and information
		Establish, document, and distribute security incident response and escalation policies
		Administration of user accounts on systems in the cardholder data network
		Monitor and control all access to cardholder data

Appendix C – Agreement to Comply with Information Security Policies

Agreement to Comply with Information Security Policies

All employees working with cardholder data must submit a signed paper copy of this form. Agency management will not accept modifications to the terms and conditions of this agreement.

I, the user, agree to take all reasonable precautions to assure that agency's internal information, or information that has been entrusted to the agency by third parties, such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with the agency, I agree to return all information to which I have had access as a result of my position with the agency. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal agency manager who is the designated information owner.

I have access to a copy of the Nebraska State Treasurer's Office Information Security Policies Manual, I have read and understand the manual, and I understand how it affects my job. As a condition of continued employment at the State agency, I agree to abide by the policies and other requirements found in that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from the agency, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password as described in the Nebraska State Treasurer's Office Information Security Policies Manual, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to the agency director and/or OCIO's office.

List what program(s) the employee has access to and why the business need for credit card information.

_____

_____

_____

_____

_____ _____

Employee's Printed Name Employee's Title

_____	_____
Employee's Telephone Number	Employee's Physical Address
_____	_____
Employee's Signature	Agency Director Signature

Appendix D – Wireless Access Point Inventory

Wireless Access Point Inventory

All agencies must maintain an inventory of all wireless access points.

Make & Model	Manufacturer	Serial Number	Mac Address	Managed By	Business Reason

Appendix E – System Inventory

Inventory Spreadsheet

Device Vendor	Device Model Name(s) and Number	Device Location	Device Status	Serial Number or Other Unique Identifier

Appendix F – Critical Technology Device Inventory

Critical Technology Device Inventory Spreadsheet

Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, email usage and internet usage. Define proper use of these technologies and the personnel approved to access.

Type	Manufacturer	Product Name	Purpose	Users with Access	Usage Approved By