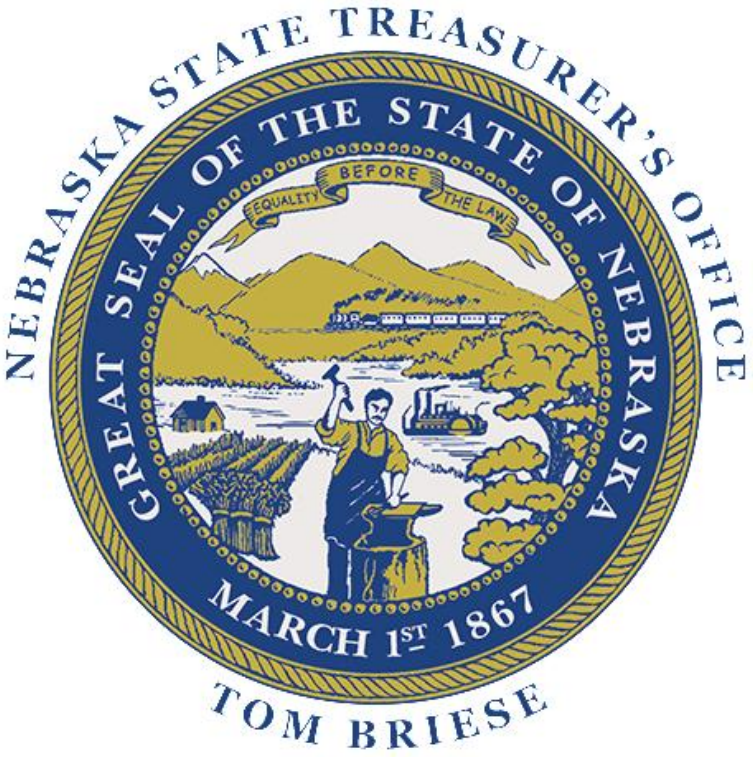

Nebraska State Treasurer's Office

Information Security Policy

Payment Card Industry Data Security Standard Compliant

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	February 15, 2017	Treasury Staff	Document created
1.1	October 16, 2017	Treasury Staff	Additional policies for specific requirements
1.2	April 15, 2024	Treasury Staff	Update to PCI version 4.0

Contents

The Nebraska State Treasurer's Information Security Policy has been updated to the Payment Card Industry Data Security Standard version 4.0. Some requirements are effective immediately and some have an effective date of March 31, 2025.

Build and Maintain a Secure Network and Systems

Section 1: Install and Maintain Network Security Controls

Network Security Controls 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. Network Security Controls examine 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, insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Network Security Controls are a key protection mechanism for any computer network.

Other system components may provide Network Security Controls functionality if they meet the minimum requirements defined. Where other system components are used within the cardholder data environment to provide Network Security Controls, these devices must be included within the scope and assessment.

Section 1.1: Processes and mechanisms for installing and maintaining network security controls (NSC)

- All security policies and operation procedures should be identified in Requirement 1 be documented, kept up to date, used by current employees with the proper roles and requirements identified. (Addresses Payment Card Industry Data Security Standard (PCI DSS) Requirement 1.1.1)
- Roles and responsibilities required are documented, assigned, and understood. (Addresses PCI DSS Requirement 1.1.2)

Nebraska Information Technology Commission's (NITC) Technical Standards and Guidelines 7-201 Network Nebraska: network edge device standard for entities choosing to connect to Network Nebraska[1] document details our policies and procedures for implementation and establishment of network security standards.

Section 1.2: NSCs are configured and maintained.

- Configuration standards for NSC rules are defined, implemented, and maintained. (Addresses PCI DSS Requirement 1.2.1)
- Changes to network connection and to configurations of NSCs are approved and managed according to Requirement 6.5.1. (Addresses PCI DSS Requirement 1.2.2)

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

Applicability Notes: Changes to network connections include the additional, removal or modification of a connection. Change to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.

- Network diagrams are detailed and maintained to show all connections between Cardholder Data Environment (CDE) and all other networks, including wireless networks. (Addresses PCI DSS Requirement 1.2.3)

Applicability Notes: A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.

- Data-flow diagram(s) which show all account data flows across systems and networks and updated when changes occur. (Addresses PCI DSS Requirement 1.2.4)

Applicability Notes: A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across systems and networks can be used to meet this requirement.

- Services, protocols, and ports allowed are identified, approved, and have a defined business need. (Addresses PCI DSS Requirement 1.2.5)
- Security features are defined and implemented for all services, protocols and ports that are in use and considered to be insecure, such that the risk is mitigated. (Addresses PCI DSS Requirement 1.2.6)
- Configuration of NSCs are reviewed at least every six months to confirm they are relevant and effective. (Addresses PCI DSS Requirement 1.2.7)
- Configuration files for NSCs are secured from unauthorized access and consistent with active network configurations. (Addresses PCI DSS Requirement 1.2.8)

Applicability Notes: Any file or setting used to configure or synchronize NSCs is considered to be a "configuration file." This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.

Section 1.3: Network access to and from the cardholder data environment is restricted.

- Inbound and outbound traffic to CDE is restricted and should be identified and determined necessary or denied. (Addresses PCI DSS Requirement 1.3.1 and 1.3.2)
- NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE,
  - All wireless traffic from wireless networks into the CDE is denied by default.
  - Only wireless traffic with an authorized business purpose is allowed into the CDE. (Addresses PCI DSS Requirement 1.3.3)
- NSCs must prohibit direct public access between the Internet and any system component in the CDE as stated in NITC 7-101 State Communication System[2]; acceptable use policy and NITC 8-101 - NITC 8-104 Information Security Policy[3].

[2] See *NITC Standards & Guidelines 7-101*

[3] See *NITC Standards & Guidelines 8-101 – 8-104*

Section 1.4: Network connections between trusted and untrusted networks are controlled.

- Network security controls must restrict connections between trusted and untrusted networks. (Addresses PCI DSS Requirement 1.4.1)
- Inbound traffic from untrusted networks to trusted networks should be restricted to communication with system components that are authorized to provide publicly accessible services, protocols, and ports. Stateful responses to communication initiated by system components in a trusted network and all other traffic is denied. (Addresses PCI DSS Requirement 1.4.2)

Applicability Notes: The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols.
This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC.

- Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network. (Addresses PCI DSS Requirement 1.4.3)
- System components that store cardholder data are not accessible from untrusted networks. (Addresses PCI DSS Requirement 1.4.4)

Applicability Notes: This requirement is not intended to apply to storage of account data in volatile memory but does apply where memory is being treated as persistent storage (for example, RAM disk). Account data can only be stored in volatile memory during the time necessary to support the associated business process (for example, until completion of the related payment card transaction).

- The disclosure of internal IP addresses and routing information is limited to only authorized parties. (Addresses PCI DSS Requirement 1.4.5)

Section 1.5: Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

- Security controls are implemented on any computing devices, including company and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows.
  - Specific configuration settings are defined to prevent threats being introduced in the entity's network.
  - Security controls are actively running.
  - Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. (Addresses PCI DSS Requirements 1.5.1)

Applicability Notes: These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not active.

This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.

Section 2: Apply Secure Configurations to All System Components

Principal requirement is updated to reflect that the focus in on secure configurations in general and not just on vendor-supplied defaults. 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: Processes and mechanisms for applying secure configurations to all system components are defined and understood.

- All security policies and operation procedures should be identified in Requirement 2 be documented, kept up to date, used by current employees with the proper roles and requirements identified. (Addresses PCI DSS Requirement 2.1.1)
- Roles and responsibilities required are documented, assigned, and understood. (Addresses PCI DSS Requirement 2.1.2) *Effective immediately.*

Section 2.2: System components are configured and managed securely.

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. NITC 8-503 Minimum server configuration[4] document, details our policies and procedures for configuration and hardening of the system.

- Configuration standards are developed, implemented, and maintained to:
  - Cover all system components.
  - Address all security vulnerabilities.
  - Consistent with industry-accepted system hardening standards or vendor hardening recommendations.
  - New vulnerability issues are identified and updated as defined in Requirement 6.3.1 Be applied when new systems are configured and verified before systems are placed into production or immediately after. (Addresses PCI DSS Requirement 2.2.1)
- 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 PCI DSS Requirement 2.2.2)

Applicability Notes: This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults.

This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.

---

[4] See *NITC Standards & Guidelines 8-503*

- ❖ Primary functions requiring different security level are managed and documented. (Addresses PCI DSS Requirement 2.2.3)
- ❖ Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled. (Addresses PCI DSS Requirement 2.2.4)
- ❖ If any insecure services, protocols, or daemons are present business justification is documented along with additional security features. (Addresses PCI DSS Requirement 2.2.5)
- ❖ System security parameters are configured to prevent misuse. (Addresses PCI DSS Requirement 2.2.6)
- ❖ Strong cryptography must be used for any non-console or web-based management interface used for administration of systems or system components. (Addresses PCI DSS Requirement 2.2.7)

Applicability Notes: This includes administrative access via browser-based interfaces and application programming interfaces (APIs).

Section 2.3: Wireless environment are configured and manage securely.

- ❖ For wireless environments connected to the cardholder data network or transmitting cardholder data all defaults will be changed. (Addresses PCI DSS Requirement 2.3.1)

Applicability Notes: This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults.

- ❖ Encryption keys or passwords 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 2.3.2)

Section 3: Protect Stored Account 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 3.1: Processes and mechanisms for protecting stored account data are defined and understood.

- ❖ All security policies and operation procedures should be identified in Requirement 3 be documented, kept up to date, used by current employees with the proper roles and requirements identified. (Addresses PCI DSS Requirement 3.1.1)
- ❖ Roles and responsibilities required are documented, assigned, and understood. (Addresses PCI DSS Requirement 3.1.2) *Effective immediately.*

Section 3.2: Storage of account data is kept to a minimum.

- ❖ Account data storage is kept to a minimum and documented through a data retention and disposal policy.
  - ➢ Policy should cover all locations of stored account data.
  - ➢ Covers sensitive authentication data (SAD) *This bullet is a best practice until its effective date of March 31, 2025, refer to Applicability Notes below for details.*
  - ➢ Legal, regulatory and/or business requirements are considered when determining retention time and data storage.

- Details length of retention period and documents business justification.
- Process for secure deletion or rendering data unrecoverable.
- Process to verify, at least once every three months, policy has been followed to securely deleted account data or rendered unrecoverable. (Addresses PCI DSS Requirement 3.2.1)

Applicability Notes: Where account data is stored bay a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted.

The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until March 31, 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.

Section 3.3: Sensitive authentication data (SAD) is not stored after authorization.

- ❖ SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. (Addresses PCI DSS Requirement 3.3.1)

Applicability Notes: Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3.

- ❖ Full track information is not retained upon completion of the authorization process. (Addresses PCI DSS Requirement 3.3.1.1)

Applicability Notes: In the normal course of business, the following data elements from the track may need to be retained:

- Cardholder name.
- Primary account number (PAN).
- Expiration date.
- Service code.

To minimize risk, store securely only these data elements as needed for business.

- ❖ Do not store the card verification code (CVV) or value (three-digit or four-digit number printed on the bank of the payment card) used to verify card-not-present transactions. (Addresses PCI DSS Requirement 3.3.1.2)

Applicability Notes: The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.

- ❖ Do not store the personal identification number (PIN) or the PIN block. (Addresses PCI DSS Requirement 3.3.1.3)

Applicability Notes: PIN blocks are encrypted during the natural course of transaction processes, but even if an entity encrypts the PIN block again, it is still not allowed to be stored after the completion of the authorization process.

- ❖ Any SAD store is encrypted using strong cryptography. (Addresses PCI DSS Requirement 3.3.2)

Applicability Notes: Whether SAD is permitted to be stored prior to authorization is determined by the organizations that manage compliance programs (for example, payment brands and acquirers). Contact the organizations of interest for any additional criteria.

This requirement applies to all storage of SAD, even if no PAN is present in the environment.

Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of authorization.

This requirement does not replace how PIN blocks are required to be managed, nor does it mean that a properly encrypted PIN block needs to be encrypted again.

This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Section 3.4: Access to displays of full PAN and ability to copy PAN is restricted.

- PAN 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[5]. (Addresses PCI DSS Requirement 3.4.1)

Applicability Notes: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment brand requirements for point-of-sale (POS) receipts.

This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.5.1 for protection of PAN when stored, processed, or transmitted.

- Document technical controls that prevent copy and/or relocation of PAN to personnel except for those with documented business need when using remote-access technologies. (Addresses PCI DSS Requirement 3.4.2).

Applicability Notes: Storing or locating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS.

This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Section 3.5: Primary Account Number (PAN) is secured whenever it is stored.

- PAN is rendered unreadable when stored by using one-way hashes based on strong cryptography, truncation, or index tokens. (Addresses PCI DSS Requirement 3.5.1)

Applicability Notes: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN.

This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected.

This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN.

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

- Hashes used to render PAN unreadable (per Requirement 3.5.1), are keyed cryptographic hashes of the entire PAN with associated key-management processes and procedure in accordance with Requirements 3.6 and 3.7. (Addresses PCI DSS Requirement 3.5.1.1)

Applicability Notes: This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected.
This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN.
This requirement is considered a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

- If disk-level or partition-level encryption (rather than file-column, or field level database encryption) is used to render PAN unreadable, it is **implemented** only as follows:
  - On removable electronic media.

OR

- If used for non-removable electronic media, PAN is rendered unreadable via another mechanism that meets Requirement 3.5.1. (Addresses PCI DSS Requirement 3.5.1.2)

Applicability Notes: While disk encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices.
Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies.
Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.
This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

- If disk-level or partition-level encryption (rather than file-column, or field level database encryption) is used to render PAN unreadable, it is **managed** as follows:
  - Logical access is managed separately and independently of native operating system authentication and access control mechanisms.
  - Decryption keys are not associated with user accounts.
  - Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely. (Addresses PCI DSS Requirement 3.5.1.3)

Applicability Notes: Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.

Section 3.6: Cryptographic keys used to protect stored account data are secured.

- Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include:
  - Access to keys is restricted to the fewest number of custodians necessary,
  - Key-encrypting keys are at least as strong as the data-encrypting keys they protect.

- Key-encrypting keys are stored separately from data-encrypting keys.
- Keys are stored securely in the fewest possible locations and forms. (Addresses PCI DSS Requirement 3.6.1)

Applicability Notes: This requirement applies to keys used to encrypt stored account data and to key-encrypting keys used to protect data-encrypting keys.
The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.

- Secret and private keys used to encrypt/decrypt sored account data are stored in one (or more) of the following forms at all times:
  - Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.
  - Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device.
  - At least two full-length key components or key shares, in accordance with an industry-accepted method. (Addresses PCI DSS Requirement 3.6.1.2)

Applicability Notes: It is not required that public keys be stored in one of these forms.
Cryptographic keys stored as part of a key-management system (KMS) that employs SCDs are acceptable.
A cryptographic key that is split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following:

• Using an approved random number generator and within an SCD,

OR

• According to ISO 19592 or equivalent industry standard for generation of secret key shares.

- Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary. (Addresses PCI DSS Requirement 3.6.1.3)
- Cryptographic keys are stored in the fewest possible locations. (Addresses PCI DSS Requirement 3.6.1.4)

Section 3.7: Where cryptography is used to protect stored account data, key-management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

- Key-management policies and procedures are implemented to include generation of strong cryptographic keys to protect stored account data. (Addresses PCI DSS Requirement 3.7.1)
- Key-management policies and procedures are implemented to include secure distribution of cryptographic keys to protect stored account data. (Addresses PCI DSS Requirement 3.7.2)
- Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data. (Addresses PCI DSS Requirement 3.7.3)
- Key-management policies and procedures are implemented for changing keys that have reach their end of their cryptoperiod, as defined by the vendor or key owner, based on industry best practice and guidelines, including a defined cryptoperiod for each key type and a process for key changes at the end of the defined cryptoperiod. (Addresses PCI DSS Requirement 3.7.4)

- ❖ Key-management policies and procedures are implemented to include the retirement, replacement, or destruction of key used to protect stored account data, when necessary:
  - ➢ Keys that have reach their end of their defined cryptoperiod.
  - ➢ Integrity of the key has been weakened, including personnel with knowledge of a cleartext key component leaves the company or the role for the key was known.
  - ➢ The key is suspected of or known to be compromised. (Addresses PCI DSS Requirement 3.7.5)
- ❖ Retired or replaced keys are not used from encryption operations.
- ❖ Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control. (Addresses PCI DSS Requirement 3.7.6)

Applicability Notes: This control is applicable for manual key-management operations or where key management is not controlled by the encryption product.

A cryptographic key that is simply split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following:

• Using an approved random number generator and within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device,

OR

• According to ISO 19592 or equivalent industry standard for generation of secret key shares

- ❖ Key-management policies and procedures are implemented to include prevention of unauthorized substitution of cryptographic keys. (Addresses PCI DSS Requirement 3.7.7)
- ❖ Key-management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept the responsibilities. (Addresses PCI DSS Requirement 3.7.8)

Section 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Strong cryptography and security protocols must be document for Cardholder data during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

Section 4.1: Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.

- ❖ All security policies and operational procedures identified in Requirement 4 must be documented, kept up to date, assigned and in use by all parties. (Addresses PCI DSS Requirement 4.1.1)
- ❖ Roles and responsibilities are documented, assigned, and understood for performing all activities. Addresses PCI DSS Requirement 4.1.2) *Effective immediately.*

Section 4.2: PAN is protected with strong cryptography during transmission.

- ❖ Strong cryptography and security protocols (NIST SP 800-52 and SP 800-57 and Publication 1800-16) must be used to protect PAN when transmitting over open, public networks. The following controls must be part of the State of Nebraska/NITC data transmission policies:

- Only trusted keys and certificates will be accepted.
- Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *The bullet is a best practice until the effective date of March 31, 2025; refer to Applicability Notes below*.
- 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).
  - In the requirement guidance for 4.2.1, "It is critical that entities maintain awareness of industry-defined deprecation dates for the cipher suites they are using and are prepared to migrate to newer versions or protocols when older ones are no longer deemed secure."
  - NIST SP 800-52 states, "It requires that TLS 1.2 configured with FIPS-based cipher suites be supported by all government TLS servers and clients and requires support for TLS 1.3 by January 1, 2024."
- The encryption strength is appropriate for the encryption methodology in use. (Addresses PCI DSS Requirement 4.2.1)

Applicability Notes: There could be occurrences where an entity receives cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of receiving sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or implement measures to prevent the channel from being used for cardholder data.
A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organization, the certificate's author is confirmed, and the certificate is verified—for example, via hash or signature—and has not expired. Note that self-signed certificates where the Distinguished Name (DN) field in the "issued by" and "issued to" field is the same are not acceptable.
The bullet above (for confirming that certificates used to safeguard PAN during transmission over open, public networks are valid and are not expired or revoked) is a best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.

- Trusted keys and certificates used to protect PAN during transmission are inventory and maintained. (Addresses PCI DSS Requirement 4.2.1.1) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.
- Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong encryption for authentication and transmission. (Addresses PCI DSS Requirement 4.2.1.2)
- PAN is secured with strong cryptography when it is sent via end-user messaging technologies. (Addresses PCI DSS Requirement 4.2.2)

Applicability Notes: This requirement also applies if a customer, or other third-party, request that PAN is sent to them via end-user messaging technologies.
There could be occurrences where an entity receives cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of receiving sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or implement measures to prevent the channel from being used for cardholder data.

Section 5: Protect All Systems and Networks from Malicious Software

Malicious software, commonly referred to as malware, enters a sensitive network segment during many businesses 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: Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

- ❖ All security policies and operational procedures identified in Requirement 5 must be documented, kept up to date, assigned and in use by all parties. (Addresses PCI DSS Requirement 5.1.1)
- ❖ Roles and responsibilities are documented, assigned, and understood for performing all activities. (Addresses PCI DSS Requirement 5.1.2*)*

Section 5.2: Malicious software (malware) is prevented or detected and addressed.

- ❖ Anti-malware solution(s) must be deployed on all systems components, except in those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware. (Addresses PCI DSS Requirement 5.2.1)
- ❖ Anti-malware solution(s) must detect, remove block, and protect against all known types of malicious software (adware, spyware, etc.). (Addresses PCI DSS Requirement 5.2.2)
- ❖ Any system components that are not at risk for malware are evaluated periodically to include a documented list of all system components, identification, and evaluation of evolving malware threats for system components, and confirmation whether such system components continue to not require anti-malware protection. (Addresses PCI DSS Requirement 5.2.3)

Applicability Notes: System components covered by this requirement are those for which there is not anti-malware solutions deployed per Requirement 5.2.1.

- ❖ Frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, performed according to all elements specified in Requirement 12.3.1.(Addresses PCI DSS Requirement 5.2.3.1) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*

Section 5.3: Anti-malware mechanisms and processes are active, maintained and monitored.

- ❖ All anti-malware solution(s) is kept current via automatic updates. (Addresses PCI DSS Requirement 5.3.1)
- ❖ All anti-malware solutions periodic scans or performs continuous behavioral analysis of systems or processes. (Addresses PCI DSS Requirement 5.3.2)
- ❖ If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. (Addresses PCI DSS Requirement 5.3.2.1)

Applicability Notes: This requirement applies to entities conduction periodic malware scans to meet Requirement 5.3.2.

This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

- For removable electronic media, the anti-malware solution(s) performs automatic scans of when the media is inserted, connected, or logically mounted or performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.

OR

- Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. (Addresses PCI DSS Requirement 5.3.3) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*
- Anti-malware solution(s) must be capable of generating audit logs and are retained in accordance with Requirement 10.5.1. (Addresses PCI DSS Requirement 5.3.4)
- Anti-malware mechanism cannot allow users to disable or alter the software unless specifically documented and authorized by management on a case-by-case basis for a limited time. (Addresses PCI DSS Requirement 5.3.5)

Applicability Notes: Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which anti-malware protection is not active.

Section 5.4: Anti-phishing mechanisms protect users against phishing attacks.

- Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. (Addresses PCI DSS Requirement 5.4.1)

Applicability Notes: This requirement applies to the automated mechanism. It is not intended that the systems and services providing such automated mechanisms (such as e-mail servers) are brought into scope for PCI DSS.

The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS.

Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa. *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*

Section 6: Develop and Maintain Secure Systems and Software

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: Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

- All security policies and operational procedures identified in Requirement 6 must be documented, kept up to date, assigned and in use by all parties. (Addresses PCI DSS Requirement 6.1.1)

- ❖ Roles and responsibilities are documented, assigned, and understood for performing all activities. (Addresses PCI DSS Requirement 6.1.2) Effective immediately.

When any vulnerability (or potential vulnerability) is found using NITC Standards & Guidelines 8-804[6] 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: Bespoke and custom software are developed securely.

- ❖ Bespoke and custom software are developed securely, based on industry standards and/or best practices for secure development, in accordance with PCI DSS requirements, such as secure authentication and logging, and incorporating consideration of information security issues during each stage of the software development lifecycle. (Addresses PCI DSS Requirement 6.2.1)

Applicability Notes: This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.

- ❖ Software development personnel working on bespoke and custom software as trained once every 12 months on software security relevant to their job function and development languages, which includes secure software design and coding techniques. If security testing tools are used, also trained on how to use the tools for detecting vulnerabilities in software. (Addresses PCI DSS Requirement 6.2.2)

Applicability Notes: Software development personnel remain knowledgeable about secure development practices; software security; and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.

- ❖ Bespoke and custom software is reviewed prior to being released into production to the customer, to identify and correct potential coding vulnerabilities.
  - ➢ Code reviews ensure code is developed according to secure coding guidelines.
  - ➢ Code reviews look for both existing and emerging software vulnerabilities.
  - ➢ Appropriate corrections are implemented prior to release. (Addresses PCI DSS Requirement 6.2.3)

Applicability Notes: This requirement for code reviews applies to all bespoke and custom software (both internal and public-facing), as part of the system development lifecycle.
Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.4.
Code reviews may be performed using either manual or automated processes, or a combination of both.

- ❖ If manual code reviews are performed for bespoke and customer software prior to release to production, code changes are required by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices, reviewed and approved by management prior to release. (Addresses PCI DSS Requirement 6.2.3.1)

Applicability Notes: Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel.

---

[6] See *NITC Standards & Guidelines 8-804* document.

An individual that has been formally granted accountability for release control and who is neither the original code author nor the code reviewer fulfills the criteria of being management.

- Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:
  - Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.
  - Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.
  - Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.
  - Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources, including cross-site scripting (XSS) and cross-site request forgery (CSRF).
  - Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.
  - Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. (Addresses PCI DSS Requirement 6.2.4)

Applicability Notes: This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.

Section 6.3: Security vulnerabilities are identified and addressed.

- Security vulnerabilities are identified and managed as follows:
  - New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
  - Vulnerabilities are assigned a risk ranking based on industry best practice and consideration of potential impact.
  - Risk ranking identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
  - Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. (Addresses PCI DSS Requirement 6.3.1)

Applicability Notes: This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.

- An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and customer software is maintained to facilitate vulnerability and patch management. (Addresses PCI DSS Requirement 6.3.2) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*

- ❖ All system components are protected from known vulnerabilities by installing applicable security patches/updates as followed:
    - ➢ Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
    - ➢ All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release). (Addresses PCI DSS Requirement 6.3.3)

Section 6.4: Public-facing web applications are protected against attacks.

- ❖ Public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:
    - ➢ Public-facing web applications must be reviewed, addressing new threats and vulnerabilities, and protected from knows attacks (using either manual or automated vulnerability security assessment tools or methods) as follows:
        - o At least once every 12 months.
        - o 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).
        - o Including all common software attacks in Requirement 6.2.4.
        - o All vulnerabilities are ranked following PCI DSS Requirement 6.3.1.
        - o All vulnerabilities must be corrected.
        - o The application is re-evaluated after corrections have been made.

OR

        - o Installing an automated technical solution that detects and prevents web-based attacks which continually checks all traffic. The solution must meet the following requirements: Is installed in front of public-facing web applications.
        - o Is actively running and updated as applicable.
        - o Is generating audit logs.
        - o Is configured to either block web-based attacks or generate an alert immediately investigated. (Addresses PCI DSS Requirement 6.4.1)

Applicability Notes: This assessment is not the same as the vulnerability scans performed for Requirement 11.3.1 and 11.3.2.

This requirement will be superseded by Requirement 6.4.2 after March 31, 2025 when Requirement 6.4.2 becomes effective.

- ❖ For public-facing web applications, an automated technical solution is deployed that continually detect and prevent web-based attacks, with at least the following:
    - ➢ Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.
    - ➢ Actively running and up to date as applicable.
    - ➢ Generating audit logs.
- ❖ Configured to either block web-based attacks or generate an alert that is immediately investigated. (Addresses PCI DSS Requirement 6.4.2)

Applicability Notes: This new requirement will replace Requirement 6.4.1 once ifs effective date is reached.

This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

- All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:
  - Method is implemented to confirm each script is authorized.
  - Method is implemented to assure that integrity of each script.
  - Inventory of all scripts is maintained with justification of why each is necessary. (Addresses PCI DSS Requirement 6.4.3)

Applicability Notes: This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties.

This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Section 6.5: Changes to all system components are managed securely.

- Changes to all system components in the production environment are made according to established procedures to include:
  - Reason for, and description of, the change.
  - Documentation of security impact.
  - Documented change approved by authorized parties.
  - Testing to verify the change does not adversely impact system security.
  - For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before deployed into production.
  - Procedures to address failures and to return to a secure site. (Addresses PCI DSS Requirement 6.5.1)
- Upon completion for a significant change all applicable PCI DSS requirement are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable. (Addresses PCI DSS Requirement 6.5.2)

Applicability Notes: These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmation activity per Requirement 12.5.2.

- Pre-production environment are separated from production environments and the separation is enforced with access controls. (Addresses PCI DSS Requirement 6.5.3)
- Roles and functions are separated between production and pre-production environment to provide accountability such that only reviewed and approved changes are deployed. (Addresses PCI DSS Requirement 6.5.4)

Applicability Notes: In environments with limited personnel where individuals perform multiple roles or functions, this same goal can be achieved with additional procedural controls that provide accountability. For example, a developer may also be an administrator that uses an administrator-level account with elevated privileges in the development environment and, for their developer role, they use a separate account with user-level access to the production environment.

- Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in account with all PCI DSS requirements. (Addresses PCI DSS Requirement 6.5.5)

- Test data and test accounts are removed before system components before the system goes into production. (Addresses PCI DSS Requirement 6.5.6)

Section 7: Restrict Access to System Components and 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: Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

- All security policies and operational procedures identified in Requirement 7 must be documented, kept up to date, assigned and in use by all parties. (Addresses PCI DSS Requirement 7.1.1)
- Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood. (Addresses PCI DSS Requirement 7.1.2) *Effective immediately.*

Section 7.2: Access to system components and data is appropriately defined and assigned.

- Access control model is defined and included granting access as follows:
  - Appropriate access depends on the entity's business and access needs.
  - Access to systems components and data resources are based on users' job classification and functions.
  - The least privileges required to perform job function. (Addresses PCI DSS Requirements 7.2.1)
- Access controls are required to enforce privileges assigned to individuals based on job classification and function. And least privileges necessary to perform job responsibilities. (Addresses PCI DSS Requirements 7.2.2)
- Required privileges are approved by authorized personnel. (Addresses PCI DSS Requirements 7.2.3).
- All user accounts and related access privilege, including third-party/vendor accounts are reviewed as follows:
  - At least once every six months
  - Ensure user accounts and access remain appropriate based on job functions.
  - Any inappropriate access is addressed.
  - Management acknowledges that access remains appropriate (Addresses PCI DSS Requirement 7.2.4)

Applicability Notes: This requirement applies to all user accounts and related access privileges, including those used by personnel and third parties/vendors, and accounts used to access third-party cloud services. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts. *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*

- All application and system accounts and related access privileges are assigned and managed as follows:
  - Based on the least privileges necessary for the operability of the system or application.
  - Access is limited to the systems, applications, or processes that specifically require their use. (Addresses PCI DSS Requirement 7.2.5) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*

- All access by application and system accounts and related access privileges are reviewed as follows:
  - Periodically (frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).
  - The application/system access remains appropriate for the function being performed.
  - Any inappropriate access is addressed.
  - Management acknowledges that access remains appropriate. (Addresses PCI DSS Requirement 7.2.5.1) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*
- All user access to query repositories of stored cardholder data is restricted as follows:
  - Via application or other programmatic methods, with access and allowed actions based on user roles and least privileges.
  - Only the responsible administrator(s) can directly access or query repositories of stored CHD. (Addresses PCI DSS Requirement 7.2.6)

Applicability Notes: This requirement applies to controls for user access to query repositories of stored cardholder data.

See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.

Section 7.3: Access to system components and data is managed via an access control system(s).

- An access control system(s) is in place that restricts access based on a user's need to know and covers all system components. (Addresses PCI DSS Requirement 7.3.1)
- The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function. (Addresses PCI DSS Requirement 7.3.2)
- The access control system(s) is set to "deny all' by default. (Addresses PCI DSS Requirement 7.3.3)

Section 8: Identify Users 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: Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

- All security policies and operational procedures identified in Requirement 8 must be documented, kept up to date, assigned and in use by all parties. (Addresses PCI DSS Requirement 8.1.1)
- Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood. (Addresses PCI DSS Requirement 8.1.2) *Effective immediately.*

Section 8.2: User identification and related accounts for users and administrators are strictly manage throughout an account's lifecycle.

- ❖ Unique IDs will be assigned for all users that access system components or cardholder data. (Addresses PCI DSS Requirement 8.2.1)

Applicability Notes: This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

- ❖ Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary and on an exception basis, and are managed as follows:
  - ➢ Accounts use is prevented unless needed for an exceptional circumstance.
  - ➢ Use is limited to the time needed for the exceptional circumstance.
  - ➢ Business justification for use is documented.
  - ➢ Use is explicitly approved by management.
  - ➢ Individual user identity is confirmed before access to an account is granted.
  - ➢ Every action taken is attributable to an individual user. (Addresses PCI DSS 8.2.2)

Applicability Notes: This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

- ❖ Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:
  - ➢ Authorized with the appropriate approval.
  - ➢ Implemented with only the privileges specified on the documented approval. (Addresses PCI DSS Requirement 8.2.4)

Applicability Notes: This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers, and third-party vendors.

- ❖ Immediately revoke access for any terminated users. (Addresses PCI DSS Requirement 8.2.5)
- ❖ Remove/disable inactive user accounts at least every 90 days. (Addresses PCI DSS Requirement 8.2.6)
- ❖ Accounts used by third parties to access, support, or maintain system components via remote access are managed to ensure they are only enabled for the time period needed, disabled when not in use, and they are monitored for unexpected activity. (Addresses PCI DSS Requirement 8.2.7)
- ❖ If a user 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 8.2.8)

Applicability Notes: This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).
This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.

Section 8.3: Strong authentication for users and administrators is established and managed.

- All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:
  - 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 element. (Addresses PCI DSS Requirement 8.3.1)

Applicability Notes: This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).
This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements.
A digital certificate is a valid option for "something you have" if it is unique for a particular user.

- Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. (Addresses PCI DSS Requirement 8.3.2)
- Verify user identity before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys.) (Addresses PCI DSS Requirement 8.3.3)
- Invalid authentication attempts are limited by:
  - Locking out the user ID after not more than 10 attempts.
  - Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. (PCI DSS Requirement 8.3.4)

Applicability Notes: This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

- If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:
  - Set to a unique value for first-time use and upon password reset.
  - Forced to be change immediately after first use. (Addresses PCI DSS Requirement 8.3.5.)
  - If passwords or passphrases are used to meet Requirement 8.3.1, a minimum level of complexity: (Addresses PCI DSS Requirement 8.3.6)
  - Require a minimum length of at least 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters)
  - Contain both numeric and alphabetic characters. (Addresses PCI DSS Requirement 8.3.6.)

Applicability Notes: This requirement is not intended to apply to:

- User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).
- Application or system accounts, which are governed by requirements in section 8.6.

This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Until March 31, 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.

- ❖ 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 8.3.7)

Applicability Notes: This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

- ❖ Authentication policies and procedures are documented and communicated to all users including:
  - ➢ Guidance on selecting strong authentication factors.
  - ➢ Guidance for how users should protect their authentication factors.
  - ➢ Instructions not to reuse previously used passwords/passphrases.
  - ➢ Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrase have been compromised **and** how to report the incident. (Addresses PCI DSS 8.3.8)
- ❖ If passwords/passphrases are used as the only authentication factor for user access, then either:
  - ➢ User passwords/passphrases are changed at least once every 90 days.

OR

  - ➢ The security posture of accounts is dynamically analyzed and real-time access to resources is automatically determined accordingly (Addresses PCI DSS Requirement 8.3.9)

Applicability Notes: This requirement applies to in-scope system components that are not in the CDE because these components are not subject to MFA requirements.
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).
This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.

- ❖ Where authentication factors such as physical or logical security token, smart cards, or certificates are used:
  - ➢ Factors are assigned to an individual user and not shared among multiple users.
  - ➢ Physical and/or logical controls ensure only the intended user can use that factor to gain access. (Addresses PCI DSS Requirement 8.3.11)

Section 8.4: Multi-factor authentication (MFA) is implemented to secure access into the CDE.

- ❖ MFA is implemented for all non-code access into the CDE for personnel with administrative access. (Addressed PCI DSS Requirement 8.4.1)

Applicability Notes: The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection—that is, via logical access occurring over a network interface rather than via a direct, physical connection.
MFA is considered a best practice for non-console administrative access to in-scope system components that are not part of the CDE.

- ❖ MFA is implemented for all access into the CDE. (Addressed PCI DSS Requirement 8.4.2)

Applicability Notes: This requirement does not apply to:

- Application or system accounts performing automated functions.

- User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting via non-console administrative access from the entity's network into the CDE.

The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.

MFA for remote access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE.

This requirement is a best proactive until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

❖ Incorporate MFA 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 8.4.3)

Applicability Notes: The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE.

If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity's networks.

The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.

Section 8.5: Multi-factor authentication (MFA) systems are configured to prevent misuse.

❖ MFA systems are implanted as follows:

- ➢ MFA system is not susceptible to replay attacks.
- ➢ MFA systems cannot be bypassed by any users, including administrative users unless specifically document, and authorized by management on an exception basis, for a limited time period.
- ➢ At least two different types of authentication factors are used.
- ➢ Success of all authentication factors is required before access is granted. (Addresses PCI DSS Requirement 8.5.1) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*

Section 8.6: Use of application and system accounts and associated authentication factors is strictly managed.

- If accounts used by systems or application can be used for interactive login, they are managed as follows:
  - Interactive use is prevented unless needed for an exceptional circumstance.
  - Interactive use is limited to the time needed for the exceptional circumstance.
  - Business justification for interactive use is documented.
  - Interactive use is explicitly approved by management.
  - Individual user identity is confirmed before access to account is granted.
  - Every action taken is attributable to an individual user. (Addresses PCI DSS Requirement 8.6.1)

    This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
- Password/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and customer source code. (Addresses PCI DSS Requirement 8.6.2)

Applicability Notes: Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2.

This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

- Password/passphrases for any application and system accounts are protected against misuse as follows:
  - Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise.
  - Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. (Addresses PCI DSS Requirement 8.6.3) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.

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 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 – 9.5)

Section 9.1: Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

- All security policies and operational procedures identified in Requirement 9 must be documented, kept up to date, assigned and in use by all parties. (Addresses PCI DSS Requirement 9.1.1)

- Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood. (Addresses PCI DSS Requirement 9.1.2) *Effective immediately.*

Section 9.2: Physical access controls manage entry into facilities and systems containing cardholder data.

- Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. (Addresses PCI DSS Requirement 9.2.1)
- Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows:
  - Entry and exit points to/from sensitive areas within the CDE are monitored.
  - Monitoring devices or mechanisms are protected from tampering or disabling.
  - Collected data is reviewed and correlated with other entries.
  - Collected data is stored for at least three months, unless otherwise restricted by law. (Addresses PCI DSS Requirement 9.2.1.1)
- Physical and/or logical controls are implemented to restrict us of publicly accessible network jacks within the facility. (Addresses PCI DSS Requirement 9.2.2)
- Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted. (Addresses PCI DSS Requirement 9.2.3)
- Access to consoles in sensitive areas is restricted via locking when not in use. (Addresses PCI DSS Requirement 9.2.4)

Section 9.3: Physical access for personnel and visitors is authorized and managed.

- Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including:
  - Identifying personnel.
  - Managing changes to an individual's physical access requirement.
  - Revoking or terminating personnel identification.
  - Limiting access to the identification process or system to authorized personnel. (Addresses PCI DSS Requirement 9.3.1)
- Physical access to sensitive areas within the CDE for personnel is control as follows:
  - Access is authorized and based on individual job function.
  - Access is revoked immediately upon termination.
  - All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination. (Addresses PCI DSS Requirement 9.3.1.1)
- Procedures are implemented for authorizing and managing visitor access to the CDE, including:
  - Visitors are authorized before entering.
  - Visitors are always escorted.
  - Visitors are clearly identified and given a badge or other identification that expires.
  - Visitor badges or other identification visibly distinguishes visitors from personnel. (Addresses PCI DSS Requirement 9.3.2)
- Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration. (Addresses PCI DSS Requirement 9.3.3)

- A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including:
    - Visitor's name and the organization represented.
    - Date and time of the visit.
    - Name of the personnel authorizing physical access.
    - Retaining the log for at least three months, unless otherwise restricted by law. (Addresses PCI DSS Requirement 9.3.4)

Section 9.4: Media with cardholder data is securely stored, accessed, distributed, and destroyed.

- All media with cardholder data is physically stored. (Addresses PCI DSS Requirement 9.4.1)
- Offline media backups with cardholder data are stored in a secure location. (Addresses PCI DSS Requirement 9.4.1.1)
- The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months. (Addresses PCI DSS Requirement 9.4.1.2)
- Add media with cardholder data is classified in accordance with the sensitivity of the data. (Addresses PCI DSS Requirement 9.4.2)
- Media with cardholder data sent outside the facility is secured as follows:
    - Media sent outside the facility is logged.
    - Media is sent by secured courier or other deliver method that can be accurately tracked.
    - Offsite tracking logs include details about media location. (Addresses PCI DSS Requirement 9.4.3)
- Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals) (Addresses PCI DSS Requirement 9.4.4)

Applicability Notes: Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have "manager" as part of their title.

- Inventory logs of all electronic media with cardholder data are maintained. (Addresses PCI DSS Requirement 9.4.5)
- Inventories of electronic media with cardholder data are conducted at least once every 12 months. (Addresses PCI DSS Requirement 9.4.5.1)
- Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:
    - Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
    - Materials are stored in secure storage containers prior to destruction. (Addresses PCI DSS Requirement 9.4.6)

Applicability Notes: These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.

- Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following:
  - The electronic media is destroyed.
  - The cardholder data is rendered unrecoverable so that is cannot be reconstructed. (Addresses PCI DSS Requirement 9.4.7)

Applicability Notes: These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.

Section 9.5: Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.

- POI devices that capture payment card data via directed physical interaction with payment card form factor are protected from tampering and unauthorized substitution, including the following:
  - Maintaining a list of POI devices.
  - Periodically inspecting POI devices to look for tampering or unauthorized substitution.
  - Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices. (Addresses PCI DSS Requirement 9.5.1)

Applicability Notes: These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped). This requirement is not intended to apply to manual PAN key-entry components such as computer keyboards.
This requirement is recommended, but not required, for manual PAN key-entry components such as computer keyboards.
This requirement does not apply to commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.

- An up-to-date list of POI devices is maintained, including:
  - Make and model of the device.
  - Location of the device.
  - Device serial number or other methods of unique identification. (Addresses PCI DSS Requirement 9.5.1.1)
- POI device surfaces are periodically inspected to detect tampering and unauthorized substitution. (Addresses PCI DSS Requirement 9.5.1.2)
  - The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed accounting to all element specified in Requirement 12.3.1. (Addresses PCI DSS Requirement 9.5.1.2.1) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.
- Training is provided for personnel is POI environments to be aware of attempted tampering or replacement of POI devices and includes:
  - Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
  - Procedures to ensure devices are not installed, replace, or returned without verification.
  - Being aware of suspicious behavior around devices.

- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel. (Addresses PCI DSS Requirement 9.5.1.3)

Section 10: Log and Monitor All Access to System Components 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: Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

- All security policies and operational procedures identified in Requirement 10 must be documented, kept up to date, assigned and in use by all parties. (Addresses PCI DSS Requirement 10.1.1)
- Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood. (Addresses PCI DSS Requirement 10.1.2) *Effective immediately.*

Section 10.2: Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

- Audit logs are enabled and active for all system components and cardholder data. (Addresses PCI DSS Requirement 10.2.1)
  - Audit logs capture all individual user access to cardholder data. (Addresses PCI DSS Requirement 10.2.1.1)
  - Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts. (Addresses PCI DSS Requirement 10.2.1.2)
  - Audit logs capture all access to audit logs. (Addresses PCI DSS Requirement 10.2.1.3)
  - Audit logs capture all invalid logical access attempts. (Addresses PCI DSS Requirement 10.2.1.4)
  - Audit logs capture all changes to identification and authentication credentials including, but not limited to:
    - Creation of new accounts.
    - Elevation of privileges.
    - All changes, additions, or deletions to accounts with administrative access. (Addresses PCI DSS Requirement 10.2.1.5)
- Audit logs capture the following:
  - All initialization of new audit logs, and
  - All starting, stopping, or pausing of the existing audit logs. (Addresses PCI DSS Requirement 10.2.1.6)
- Audit logs capture all creation and deletion of system-level objects. (Addresses PCI DSS Requirement 10.2.1.7)
- Audit logs record the following details for each auditable event:
  - User identification.
  - Type of event
  - Date and time.

- Success and failure indication.
- Origination of event.
- Identity or name of affected data, system component, resource, or service (for example, name and protocol). (Addresses PCI DSS Requirement 10.2.2)

Section 10.3: Audit logs are protected from destruction and unauthorized modifications.

- Read access to audit logs files is limited to those with a job-related need.: (Addresses PCI DSS Requirement 10.3.1)
- Audit log files are protected to prevent modifications by individuals. (Addresses PCI DSS Requirement 10.3.2)
- Audit logs file, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify. (Addresses PCI DSS Requirement 10.3.3)
- File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts. (Addresses PCI DSS Requirement 10.3.4)

Section 10.4: Audit logs are reviewed to identify anomalies or suspicious activity.

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 10.4)

- The following audit logs are reviewed at least once daily.
  - All security events.
  - Logs of all system components that store, process, or transmit CHD and/or SAD.
  - Logs of all critical system components.
  - Logs of all service and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers). (Addresses PCI DSS Requirement 10.4.1)
- Automated mechanisms are used to perform audit log reviews. (Addresses PCI DSS Requirement 10.4.1.1) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.
- Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically. (Addresses PCI DSS Requirement 10.4.2)

Applicability Notes: This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1.

- The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. (Addresses PCI DSS Requirement 10.4.2.1) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.

[7] See the *NITC Annual Risk Assessment*

- ❖ Exceptions and anomalies identified during the review process are addressed. (Addresses PCI DSS Requirement 10.4.3)

Section 10.5: Audit log history is retained and available for analysis.

- ❖ Retain audit log history for at least 12 months, with at least the most recent three moths immediately available for analysis. (Addresses PCI DSS Requirement 10.5.1)

Section 10.6: Time-synchronization mechanisms support consistent time settings across all systems.

The Nebraska State Treasurer's Office Network Time Protocol (NTP) Configuration Procedures[8] 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 10.6)

- ❖ 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 10.6.1)

Applicability Notes: Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3.

- ❖ Systems are configured to the correct and consistent time as follows:
  - ➢ One or more designated time services are in use.
  - ➢ Only the designated central time server(s) received time from external sources.
  - ➢ Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC).
  - ➢ The designated time server(s) accept time updates only from specific industry- accepted external sources.
  - ➢ Where there is more than one designated time service, the time servers peer with one another to keep accurate time.
  - ➢ Internal systems receive time information only from designated central time server(s) (Addresses PCI DSS Requirement 10.6.2)
- ❖ Time synchronization settings and data are protected as follows:
  - ➢ Access to time data is restricted to only personnel with a business need.
  - ➢ Any changes to time settings on critical systems are logged, monitored, and reviewed. (Addresses PCI DSS Requirement 10.6.3)

Section 10.7: Failures of critical security control systems are detected, reported, and responded to promptly.

- ❖ PCI DSS Requirement 10.7.1 – for services providers.
- ❖ Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:

[8] See the *Nebraska State Treasurer's Office NTP Configuration Procedures* document.

- Network security controls.
- IDS/IPS.
- Change-detection mechanisms.
- Anti-malware solutions.
- Physical access controls.
- Logical access controls.
- Audit logging mechanisms.
- Segmentation controls (if used)
- Audit log review mechanisms.
- Automated security testing tools (if used). (Addresses PCI DSS Requirement 10.7.2)

Applicability Notes: This requirement applies to all entities, including service providers, and will supersede Requirement 10.7.1 as of March 31, 2025. It includes two additional critical security control systems not in Requirement 10.7.1.

This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

❖ Failures of any critical security controls systems are responded to promptly, including but not limited to:
- Restoring security functions.
- Identifying and documenting the duration (date and time from start to end) of the security failure.
- Identifying and documenting the cause(s) of failure and documenting required remediation.
- Identifying and addressing any security issues that arose during the failure.
- Determining whether further actions are required because of the security failure.
- Implementing controls to prevent the cause of failure from reoccurring.
- Resuming monitoring of security controls. (Addresses PCI DSS Requirement 10.7.3)

Applicability Notes: This requirement applies only when the entity being assessed is a service provider until 31 March 2025, after which this requirement will apply to all entities.

This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a best practice for all other entities until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Section 11: Test Security of Systems and Networks Regularly

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

Section 11.1: Rogue Wireless Network Detection

❖ NITC Standards and Guidelines 7-105 Wireless local area network standard[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)

[9] See the *NITC Standards & Guidelines 7-105* document.

- ❖ All security policies and operational procedures identified in Requirement 11 must be documented, kept up to date, assigned and in use by all parties. (Addresses PCI DSS Requirement 11.1.1)
- ❖ Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood. (Addresses PCI DSS Requirement 11.1.2) *Effective immediately.*

Section 11.2: Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

- ❖ Authorized and unauthorized wireless access points are managed as follows:
  - ➢ The presence of wireless (Wi-Fi) access points is tested for.
  - ➢ All authorized and unauthorized wireless access points are detected and identified.
  - ➢ Testing, detection, and identification occurs at least once every three months.
  - ➢ If automated monitoring is used, personnel are notified via generated alerts. (Addresses PCI DSS Requirement 11.2.1)

Applicability Notes: The requirement applies even when a policy exists that prohibits the use of wireless technology since attackers do not read and follow company policy.
Methods used to meet this requirement must be sufficient to detect and identify both authorized and unauthorized devices, including unauthorized devices attached to devices that themselves are authorized.

- ❖ An inventory of authorized wireless access points is maintained, including a documented business justification. (Addresses PCI DSS Requirement 11.2.2)

Section 11.3: External and internal vulnerabilities are regularly identified, prioritized, and addressed.

- ❖ Internal vulnerability scans are performed as follows:
  - ➢ At least once every three months.
  - ➢ High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.
  - ➢ Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved.
  - ➢ Scan tool is kept up to date with latest vulnerability information.
  - ➢ Scans are performed by qualified personnel and organizational independence of the tester exists. (Addresses PCI DSS Requirement 11.3.1)

Applicability Notes: It is not required to use a QSA or ASV to conduct internal vulnerability scans.
Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a network administrator should not be responsible for scanning the network), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.

- ❖ All other applicable vulnerabilities (those not ranked as high-ris or critical (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:
  - ➢ Addressed based on the risk defined I the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.
  - ➢ Rescans are conducted as needed. (Addresses PCI DSS Requirement 11.3.1.1)

Applicability Notes: The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requirement 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized.
This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

- Internal vulnerability scans are performed via authenticated scanning as follows:
  - Systems unable to accept credentials for authenticated scanning are documented.
  - Sufficient privileges are used for systems accepting credentials for scanning.
  - If accounts used for authenticated canning can be used for interactive login, they are managed in accordance with Requirement 8.2.2. (Addresses PCI DSS Requirement 11.3.1.2)

Applicability Notes: The authenticated scanning tools can be either host-based or network-based.
"Sufficient" privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities.
This requirement does not apply to system components that cannot accept credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, and containers. *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.

- Internal vulnerability scans are performed after any significant change as follows:
  - High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.
  - Rescans are conducted as needed.
  - Scans are performed by qualified personnel and organizational independence of the test exists (not required to be a QSA or ASV) (Addresses PCI DSS Requirement 11.3.1.3)

Applicability Notes: Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed after significant changes.

- External vulnerability scans must be performed:
  - At least once every three months.
  - By a PCI SSC Approved Scanning Vendor (ASV).
  - Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.
  - Rescans are performed as need to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan. (Addresses PCI DSS Requirement 11.3.2)

Applicability Notes: For initial PCI DSS compliance, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s).
However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred.
ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer.

Refer to the *ASV Program Guide* published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.

- External vulnerability scans are performed after any significant change as follows:
  - Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.
  - Rescans are conducted as needed.
  - Scans are performed by qualified personnel and organizational independence of the test exists (not required to be a QSA or ASV) (Addresses PCI DSS Requirement 11.3.2.1)

Section 11.4: External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

- Implement a methodology for penetration testing that includes the following:
  - Industry-accepted penetration testing approaches. (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 6.2.4.
  - Defines network-layer penetration tests to include components that support network functions as well as operating systems.
  - Review and consideration of threats and vulnerabilities experienced in the last 12 months.
  - Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.
  - Specifies retention of penetration testing results and remediation activity results for at least 12 months. (Addresses PCI DSS Requirement 11.4.1)

Applicability Notes: Testing from inside the network (or "internal penetration testing") means testing from both inside the CDE and into the CDE from trusted and untrusted internal networks.
Testing from outside the network (or "external penetration testing") means testing the exposed external perimeter of trusted networks, and critical systems connected to or accessible to public network infrastructures.

- Internal and external penetration tests are performed:
  - Per the entities defined methodology.
  - At least once every 12 months.
  - After any significant infrastructure or application upgrade or modification.
  - By a qualified internal resource or qualified external third party.
  - Organizational independence of the tester exists (not required to be a QSA or ASV). (Addresses PCI DSS Requirement 11.4.2 & 11.4.3)
- Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows.
  - In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1

- Penetration testing is repeated to confirm the correction. (Addresses PCI DSS Requirement 11.4.4)

❖ If segmentation is used to isolate the CDE from other networks, perform penetration tests on segmentation controls.
- At least once every 12 months and after any changes to segmentation controls/methods.
- Covering all segmentation controls/methods in use.
- According to the entity's defied penetration testing methodology.
- Confirming that the segmentation controls/methods are operational and effective and isolate the CDE from all out-of-scope systems.
- Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3)
- Performed by a qualified internal resource or qualified external third party.
- Organization independence of the tester exists (not required to be a QSA or ASV) (Addresses PCI DSS Requirement 11.4.5)

Section 11.5: Network intrusion and unexpected file changes are detected and responded to.

❖ Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows.
- All traffic is monitored at the perimeter of the cardholder data environment as well as
- All traffic is monitored at critical points in the CDE.
- Personnel are alerted to suspected compromises.
- All intrusion-detection and prevention engines, baselines, and signatures are kept up to date. (Addresses PCI DSS Requirement 11.5.1)

❖ A change-detection mechanism (for example, file-integrity monitoring tools) is deployed as follows:
- To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files.
- To perform critical file comparisons at least once weekly. (Addresses PCI DSS Requirement 11.5.2)

Applicability Notes: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).

Section 11.6: Unauthorized changes on payment pages are detected and responded to.

❖ A change-and tamper-detection mechanism is deployed as follows:
- Alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.
- The mechanism is configured to evaluate the received HTTP header and payment page.
- The mechanism functions are performed as follows:
    1) At least once every seven days,

OR

- Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). (Addresses PCI DSS Requirement 11.6.1)

Applicability Notes: The intention of this requirement is not that an entity install software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described under Examples in the PCI DSS Guidance column to prevent and detect unexpected script activities.
This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Section 12: Support Information Security with Organizational Policies and Programs

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: A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

- The Nebraska State Treasurer requires that the most recent version of the information security policy be established, published, maintained, and disseminated to all relevant system users (including vendors, contractors, and business partners). (Addresses PCI DSS Requirement 12.1.1)
- The Nebraska State Treasurer's Office information security policy must be reviewed at least once every 12 months and updated as needed to reflect changes to business objectives or the risk environment. (Addresses PCI DSS Requirement 12.1.2)
- The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities. (Addresses PCI DSS Requirement 12.1.3)
- Responsibility for information security is formally assigned to Chief Information Security Officer, Internal Security Assessor, or other information security knowledgeable member of executive management. (Addresses PCI DSS Requirement 12.1.4)

Section 12.2: Acceptable use policies for end-user technologies are defined and implemented.

- Acceptable use policies for end-user technologies are documented and implemented, including:
  - Explicit approval by authorized parties.
  - Acceptable uses of the technology.
  - List of products approved by the agency for employee use, including hardware and software. (Addresses PCI DSS Requirement 12.2.1)

Applicability Notes: Examples of end-user technologies for which acceptable use policies are expected include, but are not limited to, remote access and wireless technologies, laptops, tablets, mobile phones, and removable electronic media, e-mail usage, and Internet usage.

Section 12.3: Risks to the cardholder data environment are formally identified, evaluated, and managed.

- 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.
- 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)
- Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes:
  - Identification of the assets being protected.
  - Identification of the threat(s) that the requirement is protecting against.
  - Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
  - Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.
  - Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
  - Performance of updated risk analyses when needed, as determined by the annual review. (Addresses PCI DSS Requirement 12.3.1) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.
- Cryptographic cipher suites and protocols is use are documented and reviewed at least every 12 months, including at least the following:
  - An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used.
  - Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use.
  - A documented strategy to respond to anticipated changes in cryptographic vulnerabilities. (Addresses PCI DSS Requirement 12.3.3)

Applicability Notes: The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements.

This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

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

- Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following:
  - Analysis that the technologies continue to receive security fixes from vendors promptly,
  - Analysis that the technologies continue to support (and do not preclude) the agency's PCI DSS Compliance.
  - Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology.
  - Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans. (Addresses PCI DSS Requirement 12.3.4) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.

Section 12.4: PCI DSS compliance is managed.

- Additional requirement for service providers only.

Section 12.5: PCI DSS scope is documented and validated.

- An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained, and kept current. (Addresses PCI DSS Requirement 12.5.1)
- PCI DSS scope is documented and confirmed by the agency at least once every 12 month and upon significant change to the in-scope environment.
  - Identifying all data flows for all payment stages and acceptance channels.
  - Updating data-flow diagrams per requirement 1.2.4
  - Identifying all locations where account data is stored, processed, and transmitted, including, but not limited to:
    1) Any locations outside of the currently defined CDE
    2) Applications that process CHD
    3) Transmissions between systems and networks
    4) File backups.
  - Identifying all system components in the CDE, connected to the CDE, or that could impact the security of the CDE.
  - Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.
  - Identifying all connections from third-party entities with access to the CDE.
  - Confirming that all identified data flows, account, data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. (Addresses PCI DSS Requirement 12.5.2)

Applicability Notes: This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the annual assessment.
Effective immediately.

Section 12.6: Security awareness education is an ongoing activity.

- A formal security awareness program is implemented to make all personnel aware of the agency's information security policy and procedures, and their role in protecting the cardholder data. (Addresses PCI DSS Requirement 12.6.1)
- Security awareness program is reviewed at least once every 12 months and updated as needed to address any new threats and vulnerabilities that may impact the security of CDE, or information provide to the personnel about their role in protecting cardholder data. (Addresses PCI DSS Requirement 12.6.2) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.
- Personnel receive security awareness training as following:
  - Upon hire and at least once every 12 months.
  - Multiple methods of communication are used.
  - Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures. (Addresses PCI DSS Requirement 12.6.3)
- Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to phishing and related attacks and social engineering. (Addresses PCI DSS Requirement 12.6.3.1)

Applicability Notes: See Requirement 5.4.1 in PCI DSS for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one.
This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

- Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. (Addresses PCI DSS Requirement 12.6.3.2) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.

Section 12.7: Personnel are screened to reduce risks for insider threats.

- Potential personnel who will have access to CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources. (Addresses PCI DSS Requirement 12.7.1)

Applicability Notes: For those potential personnel to be hired for positions such as store cashiers, who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.

Section 12.8: Risk to information assets associated with third-party service provider (TPSPs) relationships is managed.

- A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided. (Addresses PCI DSS Requirement 12.8.1)

Applicability Notes: The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.

- Written agreements with TPSPs are maintained as follows:
  - Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.
  - Written agreements included acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE. (Addresses PCI DSS Requirement 12.8.2)

Applicability Notes: The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement.
Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) or a declaration on a company's website) is not the same as a written agreement specified in this requirement.

- An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement. (Addresses PCI DSS Requirement 12.8.3)
- A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months. (Addresses PCI DSS Requirement 12.8.4)

Applicability Notes: Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.

- Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity. (Addresses PCI DSS Requirement 12.8.5)

Section 12.9: Third-party service providers (TPSPs) support their customers' PCI DSS compliance.

- Additional requirement for service providers only.

Section 12.10: Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

- An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. Plan includes, but is not limited to:
  - Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
  - Incident response procedures with specific containment and mitigation activities for different types of incidents.
  - Business recovery and continuity procedures.
  - Data backup processes.
  - Analysis of legal requirements for reporting compromises.

- Coverage and responses of all critical system components.
- Reference or inclusion of incident response procedures from the payment brands. (Addresses PCI DSS Requirement 12.10.1)

- At least once every 12 months, the security incident response plan is reviewed, and the content is updated as needed and tested all elements listed in Requirement 12.10.1. (Addresses PCI DSS Requirement 12.10.2)
- Specific personnel are designated to be available on a 24/7 bases to respond to suspected or confirmed security incidents. (Addresses PCI DSS Requirement 12.10.3)
- Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities. (Addresses PCI DSS Requirement 12.10.4)
- The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. (Addresses PCI DSS Requirement 12.10.4.1) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.
- The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:
  - Intrusion-detection and intrusion-prevention systems.
  - Network security controls.
  - Change-detection mechanisms for critical files. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details*.
  - The change-and tamper-detection mechanism for payment pages.
  - Detection of unauthorized wireless access points. (Addresses PCI DSS Requirement 12.10.5)

Applicability Notes: The bullet above (for monitoring and responding to alerts from a change – and tamper-detection mechanism for payment pages) is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

- The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments. (Addresses PCI DSS Requirement 12.10.6)
- The Nebraska State Treasurer's Office Incident response plan has procedures in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and included:
  - Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable.
  - Identifying whether sensitive authentication data is stored with PAN.
  - Determining where the account data came from and how it ended up where it was not expected.
  - Remediating data leaks or process gaps that resulted in the account data being where it was not expected. (Addresses PCI DSS Requirement 12.10.7) *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*

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).

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 because 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