NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Christopher J. Rein, Chief Technology Officer

P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212

www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 203-01 Information Security Payment Card Industry (PCI) Data Security Standard	**POLICY NO:** 09-05-S1-NJOIT	
	SUPERSEDES: N/A	**EFFECTIVE DATE:** 10-02-2008
	VERSION: 2.0	**LAST REVIEWED:** 02-10-2025

1 PURPOSE

The purpose of this standard is to protect sensitive credit card information and ensure compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) Version 4. This standard provides an overview of the technical and non-technical security controls that must be implemented on systems involved in processing, storing, or transmitting credit card data to safeguard against security risks associated with credit card transactions. The following are the specific names of the Payment Card Industry programs:

Mastercard's Site Data Protection (SDP)

Visa's Cardholder Information Security Program (CISP)

American Express Data Security Operating Policies (DSOP)

Discover Information Security and Compliance (DISC)

2 AUTHORITY

New Jersey Statutes Annotated (N.J.S.A.), Sections C.52:18A-224 through C.52:18A-234, known as “The Office of Information Technology Reorganization Act."

NJOIT reserves the right to change or amend this Policy to comply with changes in Agency procedures. Any changes or amendments will be announced and made available on NJOIT’s intranet under Policies. Changes in this Policy will be effective upon such publication or distribution and will not require employee sign-off.

3 SCOPE

This standard applies to all personnel including employees, temporary workers, volunteers, contractors and those employed by contracting entities, and others who store, process, or transmit credit cardholder data.

4 STANDARD

In accordance with the Statewide Information Security Manual (SISM), section RA-05: Data Classification and Security Categorization Considerations (i).

The State of New Jersey adheres to the Payment Card Industry Data Security Standard (PCI DSS) for the transmission, storage, and processing of confidential credit card data. This includes credit card magnetic stripe data, card verification values (CVV), payment account numbers (PAN), personal identification numbers (PIN), passwords, and card expiration dates. Vendors processing credit card information on behalf of the State of New Jersey are also required to comply with PCI DSS to ensure the security and confidentiality of sensitive payment card information. The State of New Jersey correspondingly adheres to the New Jersey Statewide Information Security Manual (NJSISM) https://www.cyber.nj.gov/NJ-Statewide-Information-Security-Manual.pdf .

The following is an overview of the 12 PCI DSS requirements and the corresponding NJSISM controls:

4.1 Build and Maintain a Secure Network

1. Install and Maintain a Firewall Configuration

   - Implement firewalls to protect cardholder data, ensuring that firewalls restrict connections between untrusted networks and systems in the cardholder data environment (CDE). (NJSISM SC-07)

   - Maintain firewall policies that address all connections and include incoming and outgoing traffic rules. (NJSISM SC-07)

2. Do Not Use Vendor-Supplied Defaults for System Passwords

   - Change default passwords on all systems and devices, ensuring secure access control for system configurations. (NJSISM IA-07-10)

   - Implement unique passwords and update them periodically to prevent unauthorized access. (NJSISM IA-07-10)

Protect Cardholder Data

3. Protect Stored Cardholder Data

    - Minimize the retention of cardholder data and ensure that sensitive authentication data is never stored after authorization. (NJSISM SI-12)

    - Mask card numbers when displayed (e.g., only showing the last four digits) and render PAN (Primary Account Number) unreadable through encryption, hashing, or other methods. (NJSISM SI-13)

4. Encrypt Transmission of Cardholder Data Across Open Networks

    - Use strong cryptography and encryption protocols (e.g., TLS, IPSEC) when transmitting cardholder data over public networks, including wireless, email, and messaging services. (NJSISM SC-11.1-11.2)

    - Ensure encryption keys are securely stored and managed. (NJSISM SC-10)

Maintain a Vulnerability Management Program

5. Use and Regularly Update Anti-Virus Software or Programs

    - Install and maintain antivirus software on all systems commonly affected by malware, ensuring it is regularly updated and actively monitored for threats. (NJSISM PS-15)

6. Develop and Maintain Secure Systems and Applications

    - Implement a process for identifying and applying security patches in a timely manner, ensuring that all software, including third-party applications, remains updated to address known vulnerabilities. (NJSISM RA-15)

    - Develop and follow secure coding practices to prevent security flaws such as SQL injection and cross-site scripting. (NJSISM RA-15)

Implement Strong Access Control Measures

7. Restrict Access to Cardholder Data by Business Need-to-Know

    - Limit access to cardholder data to only those individuals whose job responsibilities require it, enforcing the principle of least privilege. (NJSISM AC-10)

- Implement role-based access controls (RBAC) and regularly review access permissions. (NJSISM AC-10)

8. Identify and Authenticate Access to System Components

   - Assign a unique ID to each individual who has computer access to cardholder data, ensuring that each user is accountable for their actions. (NJSISM AC-04)

   - Implement multi-factor authentication (MFA) for access to systems that handle cardholder data. (NJSISM AC-05)

9. Restrict Physical Access to Cardholder Data

   - Implement physical access controls to restrict access to areas where cardholder data is stored, processed, or transmitted, including data centers and workstations. (NJSISM PE-07)

Regularly Monitor and Test Networks

10. Track and Monitor All Access to Network Resources and Cardholder Data

    - Implement logging mechanisms to record all access to systems and cardholder data, including administrative actions and access to critical systems. (NJSISM AU-03)

    - Regularly review logs and audit trails for unusual activity or unauthorized access. (NJSISM AU-08)

11. Regularly Test Security Systems and Processes

    - Conduct regular vulnerability assessments and penetration testing to identify weaknesses in the network and system security. (NJSISM CP-04/05)

    - Test security measures at least annually or after significant changes to ensure ongoing compliance with PCI DSS requirements. (NJSISM OR-07)

Maintain an Information Security Policy

12. Maintain a Policy That Addresses Information Security for All Personnel

    - Develop and maintain an information security policy that outlines roles, responsibilities, and expectations regarding data security. (NJSISM AT-01)

    - Ensure that all employees, contractors, and third parties are aware of the security policy and receive regular training on their responsibilities.

(NJSISM AT-01)

Compliance and Validation

To maintain PCI DSS compliance, organizations must perform regular assessments and validations:

- **Self-Assessment Questionnaires (SAQs):** Organizations may be required to complete an SAQ depending on their transaction volume and payment processing methods.
- **External Audits:** Larger organizations or service providers may be subject to annual audits conducted by a Qualified Security Assessor (QSA) to validate compliance.
- **Quarterly Scans:** Approved Scanning Vendors (ASVs) must conduct quarterly network vulnerability scans of systems involved in cardholder data environments.

Incident Response Plan

Organizations must establish and maintain an incident response plan that includes:

- **Immediate Actions:** Procedures for responding to suspected data breaches, including notification protocols for relevant stakeholders and authorities. (NJSISM IR-01-11)
- **Post-Incident Review:** Conduct a thorough investigation after an incident to identify root causes and implement measures to prevent future occurrences. (NJSISM IR-01-11)
- **Data Breach Notification:** Notify affected customers and payment card issuers if a breach occurs, as required by applicable laws and regulations. (NJSISM IR-01-11)

5 ADMINISTRATION

This Policy is administered and monitored by the CTO at 300 Riverview Plaza, Trenton, NJ 08625.

The Policy must be reviewed annually; however, the CTO reserves the right to change or amend the Policy at any time.

Signature on File 02/10/2025

Christopher J. Rein, Chief Technology Officer Date

6 DOCUMENT HISTORY

Version	Published Date	CTO	Sections Modified	Description of Modifications
1.0	10/02/2008		New	Original Published Date
2.0	02/10/2025	C. Rein	All	Updated Standard and Format