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 – Information Security Payment Card Industry (PCI) Data Security Policy	**POLICY NO:** 09-05-NJOIT	
	SUPERSEDES: N/A	**EFFECTIVE DATE:** 10-02-2008
	VERSION: 2.0	**LAST REVIEWED:** 02-10-2025

1 PURPOSE

The purpose of this policy is to safeguard sensitive credit card data and to achieve compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) Version 4. This policy establishes technical and non-technical security controls to be employed on systems used for the purpose of conducting 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

This policy is established under the authority of Policy 08-01-NJOIT, 100- Information Security Program.

OIT reserves the right to change or amend this circular to comply with changes in OIT or other agency policies.

3 SCOPE

This policy 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 POLICY

The current Payment Card Industry (PCI) Data Security Standards (DSS) Version 4 is comprised of twelve requirements organized in six logically related groups designed to enhance payment account data security. In order to achieve compliance with these requirements, all departments and agencies have the responsibility of securing the confidentiality of credit card information transmitted, stored, or used by the State of New Jersey.

Policy requirements are as follows:

4.1.1 Build and Maintain a Secure Network

4.1.1.1 Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

4.1.1.2 Do not use vendor-supplied defaults for system passwords and other security parameters.

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to comprise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

4.1.2 Protect Cardholder Data

4.1.2.1 Protect stored cardholder data

Encryption is critical component of cardholder data protection. If an intruder circumvents other network security controls and gain access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN is unencrypted e-mails.

4.1.2.2 Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

4.1.3 Maintain a Vulnerability Management Program

4.1.3.1 Use and regularly update anti-virus software or programs

Many vulnerabilities and malicious viruses enter the network via employee' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

4.1.3.2 Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that he patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerability can be avoided by using standard system development processes and security coding techniques.

4.1.4 Implement Strong Access Control Measures

4.1.4.1 Restrict access to cardholder data by business need-to-know

The requirement ensures critical data can only be accessed by authorized personnel.

4.1.4.2 Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

4.1.4.3 Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides that opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

4.1.5 Monitor and Test Networks

4.1.5.1 Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

4.1.5.2 Regularly test security systems and processes

Vulnerabilities are being discovered continually by hackers, researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

4.1.6 Main an Information Security Policy program

4.1.6.1 Maintain a policy program that addresses information security for employees and contractors.

A strong security policy program sets security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

5 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date. Failure to comply with this standard may result in disciplinary action.

6 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

7 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	Format