NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer
P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212
www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR	POLICY NO: 09-05-S1-NJOIT	
203-01 Information Security Payment Card Industry (PCI) Data Security Standard	SUPERSEDES: NEW	EFFECTIVE DATE: 10/02/2008
	VERSION: 1.0	LAST REVIEWED: 12/12/2011

ATTN: Directors of Administration and Agency IT Directors

1 PURPOSE

The purpose of this standard is to safeguard sensitive credit card data and to achieve compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.1. This standard 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 Polices (DSOP)

Discover Information Security Compliance (DISC)

2 AUTHORITY

This standard is established under the authority of Policy08-01-NJOIT, *100 – Information Security Program*.

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

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

Compliance with PCI Data Security Standard Version 1.1 is required of all merchants and service providers that store, process, or transmit credit cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. The confidentiality of credit card information must be responsibly secured during transmission and storage when in use by State of New Jersey departments and agencies.

To achieve compliance set forth in the PCI DSS Version 1.1, the following applies as a standard:

4.1 Build and Maintain a Secure Network.

4.1.1 Establish a firewall configuration that includes:

4.1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration.

4.1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks.

4.1.1.3 Requirements for a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and the Intranet.

4.1.1.4 Description of groups, roles, and responsibilities for logical management of network components.

4.1.1.5 Documented list of services/ports necessary for business.

4.1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN).

4.1.1.7 Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented.

4.1.1.8 Annual review of firewall/router rule sets.

4.1.1.9 Configuration standards for routers.

4.1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment:

4.1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:

4.1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters)

4.1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ.

4.1.3.3 Implementing stateful inspection, also known as dynamic packet filtering (only "established" connections are allowed into the network).

4.1.3.4 Placing the database in an internal network zone, segregated from the DMZ.

4.1.3.5 Restricting outbound traffic to that which is necessary for the payment card data environment.

4.1.3.6 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted), should have the same, secure configuration.

4.1.3.7 Denying all other inbound and outbound traffic not specifically allowed.

4.1.3.8 Installing perimeter firewalls between any wireless networks and the payment card data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes).

4.1.3.9 Installation of personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization's network.

4.1.4 Prohibit direct public access between external networks and any system component that stores card holder information (e.g., databases, logs, trace files).

4.1.4.1 Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic.

4.1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.

4.1.5 Implement Internet Protocol (IP) masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as Port Address Translation (PAT) or Network Address Translation (NAT).

4.2 System passwords and other security parameters.

4.2.1 Always change the vendor-supplied defaults **before** you install a system on the network (e.g., passwords, SNMP community strings, and elimination of unnecessary accounts).

4.2.1.1 For wireless environments attached to cardholder data or transmitting cardholder data, change wireless vendor defaults, including but not limited to, default service set identifier (SSID), passwords, and SNMP community strings. Enable Wi Fi Protected Access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

4.2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry best-accepted system hardening standards as defined by System Administration Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

4.2.2.1 Implement only one primary function per server (e.g., web servers, database servers, and DNS should be implemented on separate servers).

4.2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).

4.2.2.3 Configure system security parameters to prevent misuse.

4.2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

4.2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

4.2.4 Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."

4.3 Protect Cardholder Data.

4.3.1 Keep cardholder information storage to a minimum. Develop a data retention and disposal policy. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

4.3.2 Do not store sensitive authentication data subsequent to authorization (not even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 2.1 through 2.3:

4.3.2.1 Do not store the full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.).

4.3.2.2 Do not store the card-validation code (Three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data)) used to verify card-not-present transactions.

4.3.2.3 Do not store the Personal Identification Number (PIN) or the encrypted PIN block.

4.3.3 Mask Primary Account Numbers (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed).

Note that this does not apply to those employees and other parties with a specific need to see full credit card numbers.

4.3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data or portable digital media, backup media, in logs and data received from or stored by wireless networks) by using any of the following approaches:

4.3.4.1 Strong one-way hashes (hashed indexes)

4.3.4.2 Truncation

4.3.4.3 Index tokens and PADs, (pads must be securely stored).

4.3.4.4 Strong cryptography with associated key management processes and procedures.

*The **MINIMUM** account information that must be rendered unreadable is the PAN. If for some reason, a company/agency is unable to encrypt cardholder data, refer to Appendix B: "Compensation Controls for Encryption of Stored Data."*

4.3.4.5 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (e.g. by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.

4.3.5 Protect encryption keys against both disclosure and misuse.

4.3.5.1 Restrict access to keys to the fewest number of custodians necessary.

4.3.5.2 Store keys securely in the fewest possible locations and forms.

4.3.6 Fully document and implement all key management processes and procedures, including:

4.3.6.1 Generation of strong keys.

4.3.6.2 Secure key distribution.

4.3.6.3 Secure key storage.

4.3.6.4 Periodic changing of keys.

4.3.6.4.1 As deemed necessary and recommended by the associated application (e.g. re-keying) preferably automatically

4.3.6.4.2 At least annually.

4.3.6.5 Destruction of old keys.

4.3.6.6 Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key).

4.3.6.7 Prevention of unauthorized substitution of keys.

4.3.6.8 Replacement of known or suspected compromised keys.

4.3.6.9 Revocation of old or invalid keys (mainly for RSA keys)

4.3.6.10 Requirement for key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.

4.4 Encrypt transmission of cardholder and sensitive information across public networks.

4.4.1 Use strong cryptography and security protocols such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and, and Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over open public networks.

4.4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on Wired Equivalent Privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

4.4.1.1.1 Used with a minimum 104-bit encryption key and 24 bit-initialization value.

4.4.1.1.2 Use ONLY on conjunction with WiFi protected access (WPA or WPA2) technology, VPN or SSI/TLS

4.4.1.1.3 Rotate shared WEP keys quarterly (or automatically of the technology permits)

4.4.1.1.4 Rotate shared WEP keys whenever there are changes in personnel with access to keys

4.4.1.1.5 Restrict access based on media access code (MAC) address.

Note: New implementations of WEP are not allowed after March 31, 2009. Current implementations must discontinue use of WEP after June 30,2010.

4.4.2 Never send unencrypted PANs by e-mail.

4.5 Maintain a Vulnerability Management Program.

4.5.1 Deploy anti-virus software on all operating systems.

Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.

4.5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all forms of malicious software, including spyware and adware.

4.5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

4.6 Develop and maintain secure systems and applications.

4.6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

4.6.2 Establish a process to identify newly discovered security vulnerabilities (e.g. subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.

4.6.3 Develop software applications based on industry best practices and include information security throughout the software development life cycle.

4.6.3.1 Testing of all security patches and system software configuration changes before deployment.

4.6.3.2 Separate development, test, and production environments.

4.6.3.3 Separation of duties between development, test, and production environments.

4.6.3.4 Production data (live PANs) are not used for testing or development.

4.6.3.5 Removal of test data and accounts before production systems become active.

4.6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers.

4.6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.

4.6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:

4.6.4.1 Documentation of impact.

4.6.4.2 Management sign-off by appropriate parties.

4.6.4.3 Testing of operational functionality.

4.6.4.4 Back-out procedures.

4.6.5 Develop all web software and applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:

4.6.5.1 Unvalidated input.

4.6.5.2 Broken access control (e.g., malicious use of user IDs).

4.6.5.3 Broken authentication and session management (use of account credentials and session cookies).

4.6.5.4 Cross-site scripting (XSS) attacks.

4.6.5.5 Buffer overflows.

4.6.5.6 Injection flaws (e.g., structured query language (SQL) injection)

4.6.5.7 Improper error handling.

4.6.5.8 Insecure storage.

4.6.5.9 Denial of service.

4.6.5.10 Insecure configuration management.

4.6.6 All web-facing applications must be protected against known attacks by applying either of the following methods:

4.6.6.1 All application code must be reviewed for common vulnerabilities via manual or automated vulnerabilities assessment tools or methods.

4.6.6.2 Install an application layer firewall in front of web-facing applications.

4.7 Implement Strong Access Control Measures.

4.7.1 Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

4.7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

4.8 Assign a unique ID to each person with computer access.

4.8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.

4.8.2 In addition to assigning a unique ID, employ at least one of the methods to authenticate all users:

4.8.2.1 Password

4.8.2.2 Token devices (e.g., SecureID, certificates, or public key)

4.8.2.3 Biometrics

4.8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

4.8.4 Encrypt all passwords during transmission and storage on all system components.

4.8.5 Ensure proper user authentication and password management for non-consumer users and administrators, on all system components:

4.8.5.1 Control the addition, deletion, and modification of user Ids, credentials, and other identifier objects.

4.8.5.2 Verify user identity before performing password resets.

4.8.5.3 Set first-time passwords to a unique value for each user and change immediately after first use.

4.8.5.4 Immediately revoke accesses of terminated users.

4.8.5.5 Remove inactive user accounts at least every 90 days.

4.8.5.6 Enable accounts used by vendors for remote maintenance only during the time needed.

4.8.5.7 Communicate password procedures and policies to all users who have access to cardholder information.

4.8.5.8 Do not use group, shared or generic accounts and passwords.

4.8.5.9 Change user passwords at least every 90 days.

4.8.5.10 Require a minimum password length of at least seven characters.

4.8.5.11 Use passwords containing both numeric and alphabetic characters.

4.8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

4.8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.

4.8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID.

4.8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

4.8.5.16 Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users.

4.9 Restrict physical access to cardholder data.

4.9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

4.9.1.1 Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.

4.9.1.2 Restrict physical access to publicly accessible network jacks.

4.9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.

4.9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder information is accessible.

"Employee" refers to full-time and part-time employees, temporary employees/ personnel, and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

4.9.3 Make sure all visitors are handled as follows:

4.9.3.1 Authorized before entering areas where cardholder data is processed or maintained.

4.9.3.2 Given a physical token (e.g., badge or access device) that expires, and that identifies them as non-employees.

4.9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.

4.9.4 Use a visitor log to retain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.

4.9.5 Store media back-ups in a secure location preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.

4.9.6 Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain card holder information.

4.9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information including the following:

4.9.7.1 Classify the media so it can be identified as confidential.

4.9.7.2 Send the media via secured courier or a delivery method that can be accurately tracked.

4.9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).

4.9.9 Maintain strict control over the storage and accessibility of media that contains cardholder information:

4.9.9.1 Properly inventory all media and make sure it is securely stored.

4.9.10 Destroy media containing cardholder information when it is no longer needed for business or legal reasons as follows:

4.9.10.1 Crosscut shred, incinerate, or pulp hard copy materials

4.9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

4.10 Monitor and Test Networks

4.10.1 Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.

4.10.2 Implement automated audit trails for all system components to reconstruct the following events:

4.10.2.1 All individual user accesses to cardholder data.

4.10.2.2 All actions taken by any individual with root or administrative privileges.

4.10.2.3 Access to all audit trials.

4.10.2.4 Invalid logical access attempts.

4.10.2.5 Use of identification and authentication mechanisms.

4.10.2.6 Initialization of the audit logs.

4.10.2.7 Creation and deletion of system-level objects.

4.10.3 Record at least the following audit trail entries for all system components for each event:

4.10.3.1 User identification.

4.10.3.2 Type of event.

4.10.3.3 Date and time.

4.10.3.4 Success or failure indication.

4.10.3.5 Origination of event.

4.10.3.6 Identify or name of affected data, system components, or resource.

4.10.4 Synchronize all critical system clocks and times.

4.10.5 Secure audit trails so they cannot be altered.

4.10.5.1 Limit viewing of audit trails to those with a job-related need.

4.10.5.2 Protect audit trail files from unauthorized modifications.

4.10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.

4.10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.

4.10.5.5 Use file integrity monitoring/change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

4.10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example RADIUS).

Note: Log harvesting, parsing, and alerting tool may be used to achieve compliance with Requirement 10.6.

4.10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulation.

An audit history usually covers a period of at least one year, with a minimum of 3 months available online.

4.11 Regularly test security systems and processes.

4.11.1 Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts. Where wireless technology is deployed, use a wireless analyzer periodically to identify all wireless devices in use.

4.11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Note: A scan vendor qualified by the payment card industry must perform quarterly external vulnerability scans.

4.11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, sub-network added to environments, or a web server added to environment). These penetration tests must include the following:

4.11.3.1 Network-layer penetration tests

4.11.3.2 Application-layer penetration test

4.11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.

4.11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modifications of critical system or content files; and configure the software to perform critical file comparisons at least weekly.

Critical files are not necessarily those containing cardholder data. For file integrity monitoring 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. File integrity monitoring products usually come pre-configured with critical files for the related operation system. Other critical files, such as those for custom applications, must be evaluated and defined by the merchant or service provider.

4.12 Maintain an Information Security Policy Program.

4.12.1 Establish, publish, maintain, and disseminate a security policy program that:

4.12.1.1 Addresses all requirements in this specification.

4.12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.

4.12.1.3 Includes a review at least once a year and updates when the environment changes.

4.12.2 Develop daily operational security procedures that are consistent with requirements in this specification (e.g., user account maintenance procedures, log review procedures).

4.12.3 Develop usage policies for critical employee-facing technologies, such as remote access technologies, wireless technologies, removable electronic media, email usage, internet usage, laptops, and personal data assistants, to define proper use of these technologies for all employees and contractors. Ensure these usage polices require:

4.12.3.1 Explicit management approval.

4.12.3.2 Authentication for use of the technology.

4.12.3.3 A list of all such devices and personnel with access.

4.12.3.4 Labeling of devices with owner, contact information, and purpose.

4.12.3.5 Acceptable uses of the technology.

4.12.3.6 Acceptable network locations for these technologies.

4.12.3.7 A list of company-approved products.

4.12.3.8 Automatic disconnect of modem sessions after a specific period of inactivity.

4.12.3.9 Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.

4.12.3.10 When accessing cardholder data remotely via mode, disable storage of cardholder data onto local hard drives, floppy disks or other external media. Also, disable cut-and-paste and print functions during remote access.

4.12.4 Ensure the security policy program and associated standards and procedures clearly define information security responsibilities for all employees and contractors.

4.12.5 Assign to an individual or team the following information security management responsibilities:

4.12.5.1 Establish, document, and distribute security policies and procedures.

4.12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.

4.12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

4.12.5.4 Administer user accounts, including additions, deletions, and modifications.

4.12.5.5 Monitor and control all access to data.

4.12.6 Make all employees aware of the importance of cardholder information security.

4.12.6.1 Educate employees upon hire and at least annually (e.g., through posters, letters, memos, meetings and promotions).

4.12.6.2 Require employees to acknowledge in writing thy have read and understood the company's security policy and procedures.

4.12.7 Screen potential employees to minimize the risk of attacks from internal sources.

For those employees who only have access to one card number at a time to facilitate a transaction, such as store cashiers, this requirement is a recommendation only.

4.12.8 If cardholder data is shared with service providers, then contractually the following is required:

4.12.8.1 Service provider must adhere to the PCI DSS requirements.

4.12.8.2 Agreement that includes and acknowledgement that the service provider is responsible for security of cardholder data the provider possesses.

4.12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

4.12.9.1 Create an incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (e.g., informing Acquirers and credit card associations).

4.12.9.2 Test the plan at least annually.

4.12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.

4.12.9.4 Provide appropriate training to staff with security breach response responsibilities.

4.12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.

4.12.9.6 Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

4.12.10 All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:

4.12.10.1 Maintain a list of connected entities

4.12.10.2 Ensure proper due diligence is conducted prior to connecting an entity

4.12.10.3 Ensure the entity is PCI DSS compliant

4.12.10.4 Connect and disconnect entities by following an established process.

5 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this standard within 90 days of its effective date.

Failure to comply with this standard may result in disciplinary action. Requests for exceptions for non-compliance with this standard shall be processed in accordance with OIT Policy 08-02-NJOIT (*111 - Information Security Managing Exceptions*).