Weill Cornell Medicine

12.5

PCI Policy

Responsible Executive: Chief Information Officer, WCM
Original Issued: September 17, 2015
Last Updated: July 5, 2016

Policy Statement

Weill Cornell Medicine is committed to developing, adopting, and maintaining appropriate information security policies, standards, and procedures to ensure integration of information security with WCM's mission, business strategy, risk posture, and in accordance with applicable regulatory guidelines. This policy focuses on safeguarding data as it pertains to the Payment Card Industry Data Security Standard (PCI DSS).

Reason for Policy

This policy is necessary in order to maintain WCM compliance with applicable laws and standards, to protect WCM from liability, and to protect the confidentiality, integrity, and availability of WCM information systems, data, and network resources.

Entities Affected by this Policy

This policy applies to all WCM employees, contractors, service providers, and vendors. Additionally, this policy is supported by daily operational security procedures that have been developed in conjunction with this policy.

Who Should Read this Policy

All employees, contractors, service providers, and vendors of Weill Cornell Medicine who are processing credit card transactions either in electronic or paper form.

Web Address of this Policy

https://its.weill.cornell.edu/policies/

Contacts

Direct any questions about this policy, 12.5 – PCI Policy, to Brian J. Tschinkel, Information Security Officer, using one of the methods below:

- Office: (646) 962-2768
- Email: brt2008@med.cornell.edu

Contents

1. Information Security Policy

Weill Cornell Medicine is committed to developing, adopting, and maintaining appropriate information security policies, standards, and procedures to ensure integration of information security with WCM's mission, business strategy, risk posture, and in accordance with applicable regulatory guidelines.

This will be accomplished by active WCM board and management oversight, effective management and monitoring of information security risks, delineation of clear accountability for information security, and establishing appropriate organizational processes to ensure that information security risks are appropriately and regularly identified, monitored, and controlled.

This policy applies to all WCM employees, contractors, service providers, and vendors. Additionally, this policy is supported by daily operational security procedures that have been developed in conjunction with this policy.

This policy is necessary in order to maintain WCM compliance with applicable laws and standards, to protect WCM from liability, and to protect the confidentiality, integrity, and availability of WCM information systems, data, and network resources.

This policy focuses on safeguarding data as it pertains to the Payment Card Industry Data Security Standard (PCI DSS).

1.01 Roles and Responsibilities

Relevant PCI DSS 3.2 Requirements: ***12.4, 12.5 (12.5.1 – 12.5.5)***

Securing the cardholder data environment at Weill Cornell Medicine involves many teams within the Information Technologies & Services Department as well as external stakeholders. This section identifies general roles and responsibilities as it pertains to building, configuring, implementing, and maintaining WCM's cardholder data environment.

- Chief Information Officer

  The Chief Information Officer, Curtis L. Cole (ccole), provides oversight to the policies and standards in accordance with applicable laws and standards to help the organization secure Weill Cornell Medicine data and information systems. The Chief Information Officer is responsible for establishing an appropriate level of visibility for these policies and information risk to the medical college.

- ITS Associate Directors

  The ITS Associate Directors are responsible for complying with security policies within ITS. The ITS Associate Directors manage and monitor information systems that support Weill Cornell Medicine's information security infrastructure, and are responsible for maintaining awareness of the security of the resources they manage by working with the ITS Security group, and assure that security related activities are well documented and completed in a consistent and auditable manner. As directed by senior management, the ITS Associate Directors are responsible for periodic reevaluation of current operational methods to identify possible areas for improvement in security. The Information Security Officer will evaluate security risks to new and existing systems with Associate Directors in accordance with this policy. ITS Associate Directors must assure that appropriate security controls are implemented commensurate with the acceptable level of risk.

- Information Security Officer

  The Information Security Officer, Brian J. Tschinkel (brt2008), is responsible for developing and implementing strategy for security compliance within the ITS department and serves as a liaison for regulatory compliance in the medical college. The Information Security Officer develops policies, standards, and guidelines for securing information systems. In addition, the Information Security Officer conducts risk assessments and analysis in

accordance with applicable laws and standards to help the organization secure Weill Cornell Medicine data and information systems. Risk findings, including non-compliant and vulnerable systems, may be reported to the Information Security Privacy & Advisory Committee (ISPAC). The Information Security Officer reserves the right to restrict access to vulnerable systems, in accordance with the Restricting Network Access for Information Systems policy. It is the Information Security Officer's responsibility to ensure that corrective active plans are completed and information system integrity is not compromised.

- Administrators of Cardholder Data Environment

  Individuals who manage Weill Cornell Medicine's cardholder data environment are responsible for complying with policies that govern the security of the resources they manage. The Information Security Officer will establish protocols with the Systems Administrators and Systems Managers to ensure that appropriate security controls are implemented as specified in this document and related technical hardening guidelines. Systems Administrators and Systems Managers provide information to the Information Security Officer to facilitate risk assessment activities, and are responsible for implementing corrective actions as recommended. In addition, System Administrators and System Managers are responsible for maintaining sufficient documentation about system configuration, maintenance, and overall management of information systems.

  Individuals who provide access to Weill Cornell Medicine's cardholder data environment are responsible for ensuring the appropriate training and authorization requests have been completed prior to providing access. In addition, such individuals are responsible for conducting periodic access reviews as it pertains to audit and regulatory requirements.

- Department Administrators and Supervisors

  Individuals residing in the various departments, clinical sites, and other areas on the Weill Cornell Medicine campus who oversee the use of payment card processors and credit card transactions are responsible for ensuring that all individuals review and comply with the requirements set forth in this policy. In addition, these individuals are responsible for helping to maintain an adequate inventory of all equipment and serving as a point of contact for the Information Technologies & Services Department as it pertains to processing credit card transactions.

- Payment Card Processors

  All individuals responsible for handling and processing credit card payments on behalf of Weill Cornell Medicine or its affiliated entities are required to review, understand, and acknowledge the requirements set forth in this policy.

1.02 Policy Development and Maintenance

Relevant PCI DSS 3.2 Requirements: ***12.1 (12.1.1), 12.3 (12.3.1 – 12.3.10)***

This policy must be published and distributed to all appropriate WCM employees, contractors, vendors, service providers, and business partners.

This policy must be reviewed at least annually and revised as necessary, or at a time of major change to the cardholder data environment or update to the PCI DSS standards.

In addition to the requirements set forth in ITS policy *11.01 – Responsible Use of Information Technology Resources*, the following acceptable use controls must be followed to ensure proper usage of the cardholder data environment:

- Access to the systems and resources in the cardholder data environment require explicit approval and authorization by a Department Administrator. Such authorization must be in accordance with the individual's job

responsibilities, and the individual must complete the appropriate training administered by the Privacy Office and Physician Organization Information Services.

- All individuals accessing systems within the cardholder data environment must use their own uniquely assigned Center Wide ID (or "CWID") and password. No individual should access the cardholder data environment through the use of a shared or generic ID. Passwords or active sessions to any system must never be shared with another individual, as set forth in ITS policy *11.15 - Password Policy and Guidelines*.
- The Information Technologies & Services Department must maintain an inventory of all assigned credit card swipe devices and other electronic payment systems in use at various department and clinical locations. All deployed devices should be tagged in the asset management system.
- All individuals with access to the cardholder data environment must be maintained in a centralized repository. If a credit card swipe device is individually assigned, this relationship must also be maintained in the asset inventory. One individual should be designated as the appropriate contact person in order for maintenance and reconciliation of the device inventory.
- Any deployment of new products for the use of processing credit card transactions must be reviewed, assessed, and approved by the Information Technologies & Services Department. The current approved product is the ID TECH SecureKey™ M130, Encrypted Keypad with MagStripe Card Reader (IDKE-5X48XX Series).
- Cardholder data should not be copied or removed from the cardholder data environment (all data must be contained within the secure environment). Access controls must be in place to prohibit such action by any authorized individual, including access from a remote location.

1.03 Service Providers and Incident Response

Relevant PCI DSS 3.2 Requirements: ***12.8 (12.8.1 – 12.8.5), 12.9, 12.10 (12.10.1 – 12.10.6)***

A list of known service providers and a description of the service provided should be maintained centrally and reviewed for accuracy on an annual basis. The ITS Security & Identity Management team and the Physician Organization will work together to maintain this list.

The list of service providers should be reviewed on an annual basis, or at time of a significant change, to confirm that the providers are compliant with all PCI DSS standards.

The list of service providers should contain a mapping or listing of relevant PCI DSS standards that pertain to each service provider so it is clear which standards pertain to the service provider versus those which pertain to WCM.

Effective with the issuance of this policy and for all newly signed or renewed agreements, all contracts and agreements with service providers must include provisions or acknowledgement that the service providers are responsible for the security of cardholder data they either possess or otherwise store, process or transmit on behalf of WCM, or to the extent that the service providers could impact the security of WCM's cardholder data environment.

A risk assessment should be conducted for any new service providers that will be responsible for possessing, storing, or processing cardholder data on behalf of WCM. At the minimum, members of ITS Security & Identity Management, the Privacy Office, and University Counsel should be involved to adequately assess and vet the provider. The risk assessment should include a review of the service providers' policies that demonstrate their commitment to comply with PCI DSS standards.

In accordance with ITS policy *11.05 – Security & Privacy Incident Response Plan* and the WCM Security & Privacy Incident Response Team (SPIRT), the WCM Security & Privacy Incident Response Plan must be tested annually and include reporting requirements in the event of a suspected incident or breach involving cardholder data. The WCM Security & Privacy Incident Response Plan includes appropriate provisions for reporting and escalating incidents pertaining to the cardholder data environment and is the authoritative plan as it pertains to this policy document.

2. Secure Network and Systems

2.01 Firewall Configuration

Relevant PCI DSS 3.2 Requirements: ***1.1 (1.1.1 – 1.1.7), 1.2 (1.2.1 – 1.2.3), 1.3 (1.3.1 – 1.3.7), 1.4 – 1.5***

WCM must develop and implement formal, documented standards for its firewalls and routers. Such standards must include:

- A formal process for approving and testing all network connections and changes to WCM firewall and router configurations
- A current network diagram that identifies all connections between WCM's cardholder data environment and other networks, including any wireless networks
- A current diagram that shows all WCM's cardholder data flows across systems and networks; the diagram must be kept current and updated as needed upon changes to the environment
- Requirements for a firewall at each internet connection and between any demilitarized zone (DMZ) and WCM's internal network zone
- A description of groups, roles, and responsibilities for management of WCM's network components
- Documentation and business justification for use of all services, protocols, and ports allowed by WCM's firewalls and routers, including documentation of security features implemented for those protocols considered to be insecure (e.g., FTP, Telnet, POP3, IMAP, and SNMP v1 and v2)
- A requirement to review WCM's firewall and router rule sets at least every six (6) months

WCM firewall and router configurations must restrict connections between untrusted networks and any system components in the WCM cardholder data environment. Such configurations must:

- Restrict inbound and outbound traffic to that which is necessary for WCM's cardholder data environment, and specifically deny all other traffic
- Secure and synchronize configuration files across routers and firewalls
- Configure perimeter firewalls between all wireless networks and WCM's cardholder data environment, to deny or—if traffic is necessary for business purposes—permit only authorized traffic between the wireless environment and WCM's cardholder data environment
- Prohibit direct public access between the internet and any system component in WCM's cardholder data environment, such that
- A DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports

- Inbound internet traffic is limited to IP addresses within the DMZ
- Direct connections inbound or outbound for traffic between the internet and WCM's cardholder data environment are not allowed
- Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering WCM's network
- Unauthorized outbound traffic from WCM's cardholder data environment to the internet is not allowed
- A stateful inspection (or dynamic packet filtering) firewall is implemented to allow only "established" connections into WCM's network
- System components storing WCM cardholder data should be placed in one of WCM's internal network zones (such as "high") and should be segregated from WCM's DMZ and any other untrusted networks
- Private WCM IP addresses and other internal routing information are not disclosed to unauthorized parties (e.g., masquerading via implementation of NAT, proxies, etc.)
- Personal host-based firewalls or equivalent software are installed on any mobile device or computer containing, storing, accessing, or transmitting WCM data over the internet; these firewalls need to be configured to prevent unauthorized users from altering or disabling the firewall

> Weill Cornell Physician Network (WCPN) sites that are accepting credit card transactions are in-scope of the greater cardholder data environment. In order to comply with the above requirements to secure the cardholder data environment, all WCPN sites are required to have an active metropolitan-area Ethernet ("metro Ethernet") connection with WCM. WCPN sites configured with a local internet or virtual private network (VPN) connection will not be able to comply with the above requirements. In these cases, a remediation plan must be established and agreed upon by ITS Security, the Physician Organization, and the WCPN site to implement a metro Ethernet connection within six (6) months.

2.02 Default System and Security Parameters

Relevant PCI DSS 3.2 Requirements: ***2.1 (2.1.1), 2.2 (2.2.1 – 2.2.5), 2.3 – 2.6***

In accordance with ITS policy *11.11 - Requirements for Securing Information Systems*, the following configuration items must ensure that:

- Vendor default passwords and other vendor default settings are changed prior to system implementation in order to prevent a system from being compromised by malicious individuals making use of standard configuration parameters
- Default settings for any wireless environments connected to WCM's cardholder data environment must also be changed, including, but not limited to:
    - encryption keys
    - shared passwords and administrator passwords
    - SNMP community strings
    - Servers are configured for one purpose, only

- Only necessary services, protocols, daemons, etc. as required for the system's business purpose are enabled
- Additional security controls are enabled for insecure services

All systems in-scope for WCM's cardholder data environment must be inventoried and updated accordingly.

3. Protect Cardholder Data

3.01 Protection of Stored Cardholder Data

Relevant PCI DSS 3.2 Requirements: ***3.1, 3.2 (3.2.1 – 3.2.3), 3.3***

As WCM has implemented end-to-end encryption for its transmission of cardholder data, no digital cardholder data shall be stored after authorization in the WCM cardholder data environment. For situations where cardholder data is collected in a paper format, the following controls must be adhered to:

- Paper documents containing cardholder data must be redacted of sensitive authentication data (full track data, card validation code or value, and PIN data) after the credit card has been authorized.
- All redacted paper documents may be retained in accordance with the institution or department's data retention policies.
- Any retained paper documents should be reviewed on a quarterly basis and documents older than the retention period must be securely shredded.
- In situations where the cardholder's primary account number (PAN) is displayed, the PAN must be masked such that only the first six or last four digits are displayed. Only personnel with a legitimate business need shall have the authorizations to review the full PAN.

3.02 Encryption of Transmitted Cardholder Data

Relevant PCI DSS 3.2 Requirements: ***4.1 (4.1.1), 4.2, 4.3***

The WCM cardholder data environment must be isolated and segregated from the rest of the WCM network. In addition, there is no access to the WCM cardholder data environment from unsecure networks, including any wireless technologies.

- Any transmission of cardholder data must be encrypted using strong cryptography and security protocols. The encryption standard must be approved by the Information Technologies & Services Department.
- For any browser-based transactions of cardholder data, the system must be configured to utilize HTTP Secure, over **TLS version 1.2 or greater**, for encryption. **All versions of SSL are considered weak encryption mechanisms and must not be used.**
- In accordance with ITS policy *11.08 – Use of Email* and ITS policy *11.09 – Data Loss Prevention (DLP)*, cardholder data must never be sent unprotected via email, text message, instant messaging, chat, or other communication protocols. **It is strongly recommended to never send sensitive authentication data through these protocols, even with added encryption.**

4. Vulnerability Management

4.01 Malware Protection

Relevant PCI DSS 3.2 Requirements: ***5.1 (5.1.1, 5.1.2), 5.2 – 5.4***

While there are several security monitoring tools to detect and protect against the presence of malware (malicious software, including viruses, worms, and Trojans) on the WCM network, the cardholder data environment must be configured and monitored accordingly to protect against malware infections.

- The ITS-approved antivirus software must be deployed, configured, and activated on all workstations and servers within the cardholder data environment that are handling or processing cardholder data.
- All antivirus clients must be current (within 3 update revisions) with the latest definition updates and rulesets.
- The antivirus software must be configured to generate audit logs at time of detection or quarantine of malware.
- The antivirus software must be capable of performing a periodic scan if initiated by the system administrator.
- The antivirus software must be configured in such a way to prevent other users of the system from disabling or altering the configuration settings.
- Any exceptions or exclusions that result in a temporary or permanent change to the antivirus software must be submitted to ITS Security for review and implementation.

4.02 Secure Systems and Applications

Relevant PCI DSS 3.2 Requirements: ***6.1, 6.2***

In order to maintain a secure environment, ITS Security runs automated vulnerability scans of all systems within the cardholder data environment.

The vulnerability scanning tool is configured such that:

- All systems within the cardholder data environment are scanned on a weekly basis
- All systems are categorized and assessed with a risk score based on sensitivity of data, exposure to threats, and likelihood of compromise – all of which are compiled based on outside security metrics and threat bulletins

In addition, all systems are patched with the latest security updates on a monthly basis. In accordance with ITS policy *11.12 - Restricting Network Access for Insecure Systems*, any system that appears to be vulnerable to a threat and has a high likelihood of compromise may be blocked by ITS from accessing the network, including the internet.

5. Access Control

5.01 Logical Access Control Measures

Relevant PCI DSS 3.2 Requirements: ***7.1 (7.1.1 – 7.1.4)***

In accordance with ITS policy *12.3 - Authentication and Authorization*, cardholder data can only be accessed by authorized personnel. Access to the cardholder data environment must be restricted on a “need to know” basis to only authorized individuals based on role, job function, and responsibility.

Individuals which process clinical-related cardholder data must complete the appropriate training courses offered by the Physician Organization in order to gain access to the electronic medical record payment modules. Such users must be authorized by a supervisor in order to complete the training in accordance with their job functions and responsibilities.

Users that do not require access to the cardholder data environment must not be permitted to gain access without proper authorization, Active Directory group membership, or other application and network access control measures.

Access to the cardholder data environment should be reviewed and recertified on an annual basis to ensure authorizations are accurate and reflect current responsibilities.

5.02 Authentication to System Components

Relevant PCI DSS 3.2 Requirements: ***8.1 (8.1.1 – 8.1.8), 8.2 (8.2.1 – 8.2.6), 8.3 – 8.5 (8.5.1), 8.6, 8.8***

All individuals accessing the cardholder data environment must comply with the requirements set forth in ITS policy *12.3 – Authentication and Authorization* and the ITS policy *11.15 - Password Policy and Guidelines*.

The following controls and requirements apply to vendors or other third parties supporting and/or requiring access to the cardholder data environment:

- Vendors must access the cardholder data environment using a uniquely-assigned account
- The uniquely-assigned vendor accounts must be granted access to only the roles and modules required for the purposes of support (“need to know” method)
- All vendor accounts must be recertified by ITS Security on a quarterly basis; sign-off is required by the vendors’ sponsor in order to maintain access to the system
- Vendor accounts must only be enabled when required for troubleshooting a support request or responding to an incident; accounts can be enabled through the use of a support ticket with ITS Security
- A shared session should be used when a vendor must connect to the cardholder data environment via remote access; if this is not feasible, audit logs may be reviewed at any time by ITS Security in the event suspicious or malicious activity has occurred

Individuals responsible for administering the cardholder data environment must enroll in and utilize WCM’s multifactor authentication technology before interactively logging in to a server or system. Remote connections to the cardholder data environment (including those established by vendor support personnel) must also utilize multifactor authentication for added security.

5.03 Physical Access Control Measures

Relevant PCI DSS 3.2 Requirements: ***9.1.2, 9.5, 9.6 (9.6.1 – 9.6.3), 9.7, 9.8 (9.8.1), 9.9 (9.9.1 – 9.9.3)***

In addition to the requirements set forth in ITS policy *12.2 – Physical Security*, the following controls must be adhered to in order to ensure adequate physical security around cardholder data:

- Network jacks or wireless access points located in public areas and areas accessible to visitors must not provide access to the dedicated cardholder data environment virtual local area network (VLAN).
- Any media containing high risk data, as defined in ITS policy *11.03 – Data Classification*, which includes cardholder data, must be physically secured to prevent unauthorized access or disclosure.

- Confidential data must never be left in plain sight. Workstations must be locked when left unattended and cardholder data stored in paper format must be securely stored and locked when unattended.
- The data loss prevention system, as defined in ITS policy *11.09 – Data Loss Prevention (DLP)*, must be configured to detect and alert on credit card numbers transmitted via email, the network, or in digital format to a removable storage device. Cardholder data must never be transmitted through email. Under extreme circumstances, any data must be sent using encryption, as defined in ITS policy *11.08 – Use of Email*.
- An inventory of cardholder data must be maintained, such that the location of cardholder data in electronic and paper formats is known (e.g., specific storage closets, cabinets, servers, or data centers).
- All media containing cardholder data must be destroyed when it is no longer needed for business or legal reasons. As defined in ITS policy *12.2 – Physical Security* and *NIST Special Publication 800-88 Revision 1 Guidelines for Media Sanitization*, media must be destroyed using an approved technique (disintegrate, pulverize, melt, incinerate, or shred) to ensure cardholder data is not recoverable.
- Devices that capture payment card data via direct physical interaction with the card (e.g., a card swipe or dip device) must be protected from tampering or substitution.
    - Where possible, card swipe devices should be removed at the end of the business day and securely stored in a locked cabinet or office to protect against tampering or substitution.
        - If card swipe devices cannot be removed, disconnected, and securely stored, they should be inspected for tampering or substitution at the start of each business day.
        - Card swipe devices should be inspected based on the following standards:
        - Validate the manufacturer's name and model number are correct.
        - Validate the serial number against the department's inventory.
        - Validate the manufacturer's security seals and labels are present with no signs of peeling or tampering.
        - Validate the device's color and condition are as expected, with no additional marks or scratches around the seams, reader, or window display.
- All individuals interacting with credit cards and card swipe devices should be aware of and trained against the requirements set forth in this policy to ensure devices have not been tampered with or substituted.

6. Network Monitoring and Testing

6.01 Monitoring of Network Resources

Relevant PCI DSS 3.2 Requirements: ***10.1, 10.2 (10.2.1 – 10.2.7), 10.3 (10.3.1 – 10.3.6), 10.5, 10.6 (10.6.1 – 10.6.3), 10.7, 10.9***

All critical system and network components within the cardholder data environment should be configured to track and record audit logs that link individuals to actions. Logs should be forwarded to the ITS centralized security information and event manager (SIEM) to ensure they are (a) tracked, reviewed, and monitored daily, and (b) stored in a secure location where they cannot be modified.

Automated logs should include the following events in order to reconstruct a timeline in the event of an incident or investigation:

- All individual user accesses to cardholder data, whether at the operating system or application level
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails by any individual
- Individual or denied access attempts, such as failed or bad password
- Use of and changes to authentication mechanisms, such as creating new accounts, elevating user privileges, etc.
- Initialization, stopping, or pausing of the audit logs
- Creation and deletion of system-level objects

All system components within the cardholder data environment should record the following events in system audit logs:

- User account or identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

Any errors, anomalies, or suspicious entries must be reviewed and escalated according to standard incident response processes and procedures. All audit log entries, specific to the cardholder data environment, must be retained for at least one year, with a minimum of three months immediately available for analysis.

6.02 Security System and Process Testing

Relevant PCI DSS 3.2 Requirements: ***11.2 (11.2.1 – 11.2.3), 11.3 (11.3.1 – 11.3.4), 11.5 (11.5.1), 11.6***

System components, processes, and applications need to be tested frequently to ensure security controls continue to reflect a changing environment.

- Vulnerability scans must be run at least quarterly and after any significant change in the network which impacts the cardholder data environment (such changes may include new system component installations, changes in network topology, firewall rule modifications, or product upgrades)
- Internal quarterly vulnerability scanning must be performed by members of the ITS Security team (“qualified personnel”)
- Internal quarterly vulnerability scans must be repeated until all “high-risk” vulnerabilities are resolved, remediated, and/or exempted (requires ITS Security approval)

- External quarterly vulnerability scanning must be performed by an Approved Scanning Vendor (ASV)—presently, Rapid7—approved by the Payment Card Industry Security Standards Council (PCI SSC)
- External quarterly vulnerability scans must be repeated until all “high-risk” vulnerabilities are resolved, remediated, and/or exempted (requires ITS Security approval)

In order to continually assess the cardholder data environment, penetration testing (both internal and external) must be conducted by a qualified external security services firm every six months or after any significant infrastructure or application upgrade or modification. Penetration testing should include the following:

- Based on industry-accepted penetration testing approaches, such as NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment
- Coverage of the entire cardholder data environment perimeter and critical systems and applications
- Testing from both inside and outside the network
- Testing to validate all out-of-scope systems are segmented from systems in the cardholder data environment
- 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

Any application-layer penetration tests for commercial “off-the-shelf” products need to be coordinated in conjunction with the software vendor. All penetration testing results and remediation activities must be maintained by ITS Security.
In accordance with ITS policy *11.11 - Requirements for Securing Information Systems*, the cardholder data environment must be secured with intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. In addition, change-detection software must be installed and configured on cardholder data systems to detect unauthorized changes, additions, and deletions of critical system files.

ITS Security must be able to receive and monitor alerts for traffic at the perimeter of the cardholder data environment as well as at critical points within the environment. Signatures, definitions, engines, and agents must be current with ITS standard builds and deployments.

7. Additional Resources

The following ITS policies are referenced:

- 11.01 – Responsible Use of Information Technology Resources
- 11.03 – Data Classification
- 11.05 – Security & Privacy Incident Response Plan
- 11.08 – Use of Email
- 11.09 – Data Loss Prevention
- 11.11 – Requirements for Securing Information Systems
- 11.12 – Restricting Network Access for Insecure Systems

- 11.15 – Password Policy and Guidelines
- 12.2 – Physical Security Policy
- 12.3 – Authentication and Authorization

The following referenced guidelines are available on the NIST website:

- NIST Special Publication 800-88 Revision 1 Guidelines for Media Sanitization
- NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment

The following additional resources are available on the PCI website:

- Glossary of Terms, Abbreviations, and Acronyms v3.2
- PCI DSS v3.2
- SAQ C v3.2

Appendix A: Definitions

These definitions apply to institutions and regulations as they are used in this policy.

- WCM — Weill Cornell Medicine
- ITS — Information Technologies & Services Department

The following terms and abbreviations are relevant to this policy, as defined by the Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS):

- antivirus — Program or software capable of detecting, removing, and protecting against various forms of malicious software (also called “malware”) including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits.
- audit log — Also referred to as “audit trail.” Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
- authentication — Process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as: 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
- authorization — In the context of access control, authorization is the granting of access or other rights to a user, program, or process. Authorization defines what an individual or program can do after successful authentication. In the context of a payment card transaction, authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
- card skimmer — A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.
- cardholder — Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
- cardholder data — At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code
- CDE — Acronym for “cardholder data environment.” The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
- compromise — Also referred to as “data compromise,” or “data breach.” Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.

• default accounts	Login account predefined in a system, application, or device to permit initial access when system is first put into service. Additional default accounts may also be generated by the system as part of the installation process.
• default password	Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.
• DSS	Acronym for “Data Security Standard.”
• encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.
• firewall	Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
• FTP	Acronym for “File Transfer Protocol.” Network protocol used to transfer data from one computer to another through a public network such as the internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology.
• HTTP	Acronym for “hypertext transfer protocol.” Open internet protocol to transfer or convey information on the World Wide Web.
• HTTPS	Acronym for “hypertext transfer protocol over secure socket layer.” Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as web-based logins.
• IDS	Acronym for “intrusion-detection system.” Software or hardware used to identify and alert on network or system anomalies or intrusion attempts. Composed of: sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to detected security events.
• IPS	Acronym for “intrusion prevention system.” Beyond an IDS, an IPS takes the additional step of blocking the attempted intrusion.
• LAN	Acronym for “local area network.” A group of computers and/or other devices that share a common communications line, often in a building or group of buildings.
• least privilege	Having the minimum access and/or privileges necessary to perform the roles and responsibilities of the job function.

• malicious software	Also known as “malware.” Software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner’s data, applications, or operating system. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
• merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
• monitoring	Use of systems or processes that constantly oversee computer or network resources for the purpose of alerting personnel in case of outages, alarms, or other predefined events.
• multifactor authentication	Method of authenticating a user whereby two or more factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints, other forms of biometrics, parametrics, etc.).
• network components	Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
• network security scan	Process by which an entity’s systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals.
• network segmentation	Also referred to as “segmentation” or “isolation.” Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment.
• NIST	Acronym for “National Institute of Standards and Technology.” Non-regulatory federal agency within U.S. Commerce Department's Technology Administration.

• off-the-shelf	Description of products that are stock items not specifically customized or designed for a specific customer or user and are readily available for use.
• PA-DSS	Acronym for “Payment Application Data Security Standard.”
• PAN	Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
• password	A string of characters that serve as an authenticator of the user.
• patch	Update to existing software to add functionality or to correct a defect.
• payment application	In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties.
• payment cards	For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.
• payment processor	Sometimes referred to as “payment gateway” or “payment service provider (PSP)”. Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand.
• PCI	Acronym for “Payment Card Industry.”
• PCI DSS	Acronym for “Payment Card Industry Data Security Standard.”
• penetration test	Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the environment (external testing) and from inside the environment.
• PIN	Acronym for “personal identification number.” Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature.
• privileged user	Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. However, the extent of privileges across different privileged accounts can vary greatly depending on the organization, job function or role, and the technology in use.

• QSA	Acronym for “Qualified Security Assessor.” QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments.
• RADIUS	Abbreviation for “Remote Authentication Dial-In User Service.” Authentication and accounting system. Checks if information such as username and password that is passed to the RADIUS server is correct, and then authorizes access to the system. This authentication method may be used with a token, smart card, etc., to provide multifactor authentication.
• remote access	Access to computer networks from a location outside of that network. Remote access connections can originate either from inside the company’s own network or from a remote location outside the company’s network. An example of technology for remote access is VPN.
• removable electronic media	Media that store digitized data and which can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives and removable hard drives.
• router	Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.
• SAQ	Acronym for “Self-Assessment Questionnaire.” Reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.
• secure wipe	Also called “secure delete,” a method of overwriting data residing on a hard disk drive or other digital media, rendering the data irretrievable.
• security event	An occurrence considered by an organization to have potential security implications to a system or its environment. In the context of PCI DSS, security events identify suspicious or anomalous activity.
• sensitive authentication data	Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.
• service code	Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
• service provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other

	entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).
• SSL	Acronym for “Secure Sockets Layer.” Industry standard that encrypts the channel between a web browser and web server. Now superseded by TLS. See *TLS.*
• stateful inspection	Also called “dynamic packet filtering.” Firewall capability that provides enhanced security by keeping track of the state of network connections. Programmed to distinguish legitimate packets for various connections, only packets matching an established connection will be permitted by the firewall; all others will be rejected.
• system components	Any network devices, servers, computing devices, or applications included in or connected to the cardholder data environment.
• threat	Condition or activity that has the potential to cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization.
• TLS	Acronym for “Transport Layer Security.” Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
• track data	Also referred to as “full track data” or “magnetic-stripe data.” Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.
• virtual payment terminal	A virtual payment terminal is web-browser-based access to an acquirer, processor or third party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
• VLAN	Abbreviation for “virtual LAN” or “virtual local area network.” Logical local area network that extends beyond a single traditional physical local area network.
• VPN	Acronym for “virtual private network.” A computer network in which some of connections are virtual circuits within some larger network, such as the internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public internet, a VPN may or may not have strong security features such as

	authentication or content encryption. A VPN may be used with a token, smart card, etc., to provide multifactor authentication.
• vulnerability	Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system.
• web application	An application that is generally accessed via a web browser or through web services. Web applications may be available via the internet or a private, internal network.