2018 SecurityMetrics Guide to

PCI DSS COMPLIANCE

IT CHECKLISTS

securityMETRICS®

REQUIREMENT 1 IT CHECKLIST

FIREWALL IMPLEMENTATION AND REVIEW

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ Firewall
- ☐ "Deny All" rule for all other inbound and outbound traffic (1.2.1b)
- ☐ Stateful inspection/dynamic packet filtering (1.3.5)
- ☐ Documented business justification for each port or protocol allowed through the firewall (1.1.6a)

THINGS YOU WILL NEED TO DO:

- ☐ Limit traffic into the CDE to that which is necessary (1.2.1.a)
- ☐ Position firewall to prohibit direct inbound and outbound traffic from the CDE (1.3)
- ☐ Create secure zone for any card data storage, which must be separate from DMZ (1.3.6)
- ☐ Explicitly authorize outbound connections from the CDE (1.3.4)
- ☐ Document all firewall policies and procedures (1.2.1.a, 1.2.1.b, 1.2.3, 1.3, 1.3.3, 1.3.5, 1.3.6)

THINGS YOU MAY NEED TO DO:

- ☐ Install a firewall between wireless networks and the CDE (wireless only) (1.2.3)

REQUIREMENT 2 IT CHECKLIST

CONFIGURATION STANDARDS

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ A secure way to access and manage systems in your environment (2.3)
- ☐ An inventory of all hardware and software used in the CDE
- ☐ Documented configuration standards for all types of systems in the CDE

THINGS YOU WILL NEED TO DO:

- ☐ Assign system administrator and/or knowledgeable personnel the responsibility of configuring system components (2.2.4)
- ☐ Implement a system hardening guide covering all components of the CDE (2.2.a)
- ☐ Disable and uninstall any unnecessary programs, services, guest accounts, scripts, drivers, features, subsystems, file systems, and web servers. Document which services and programs are allowed (2.2.2, 2.2.3, 2.2.5)
- ☐ Change vendor-supplied default usernames and passwords. Remove or disable unnecessary default accounts before installing a system on the network (e.g., operating systems, security software, POS terminals, routers, firewalls, SNMP) (2.1.a, 2.1.b, 2.1.1.b, 2.1.1.c, 2.1.1.d, 2.1.1.e)
- ☐ Document security policies and operation procedures for managing vendor defaults and other security settings. Inventory all systems within scope of the payment application environment and keep inventory up to date (2.4, 2.5)

THINGS YOU MAY NEED TO DO:

- ☐ Use technologies such as VPN for web-based management and other non-console administrative access. Ensure all traffic is encrypted following current standards (2.1.1.d, 2.3)
- ☐ If wireless Internet is enabled in the CDE, change wireless default settings including encryption keys, passwords, and SNMP community strings (2.1.1)
- ☐ Enable only one primary function per server (e.g., logging server, web server, DNS) (2.2.1)

REQUIREMENT 3 IT CHECKLIST

SECURING CARDHOLDER DATA

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ A documented data retention policy
- ☐ A data flow diagram

THINGS YOU WILL NEED TO DO:

- ☐ Have employees acknowledge their training and understanding of the policy (3.1, 3.6.8, 3.7)
- ☐ Eliminate storage of sensitive authentication data after card authorization (3.2.d, 3.2.1, 3.2.2, 3.2.3)
- ☐ Mask out PAN on customer receipts (3.3)
- ☐ Understand guidelines for handling and storing cardholder data

THINGS YOU MAY NEED TO DO:

- ☐ If PAN data is stored for business or legal reasons, details must be masked, truncated, or secured by strong cryptography (3.4)
- ☐ PAN storage should be accessible by as few employees as possible for business or legal reasons. This includes limited access to cryptographic keys, removable media, or hardcopy of stored details (3.4.1, 3.5, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7)

REQUIREMENT 4 IT CHECKLIST

TRANSMITTING CARDHOLDER DATA

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- [ ] An in-house policy to ensure you do not send unprotected PANs via end-user messaging technologies (4.2.b)

THINGS YOU WILL NEED TO DO:

- [ ] Check all related device configuration for proper encryption. Check with vendors to make sure supplied POS/POI devices are encrypting data appropriately (Appendix A2)
- [ ] Validate that POS/POI devices are not susceptible to any known exploits. Devices and software used to process credit cards need to be PCI DSS compliant (Appendix A2.1)
- [ ] Review all locations where CHD is transmitted or received. Examine system configurations. Review all devices/systems to ensure you use appropriate encryption within your CDE. You must safeguard sensitive cardholder data during transmission over open, public networks (4.1, 4.1.1)
- [ ] Use only trusted keys and/or certificates. Check inbound/outbound transmissions and verify that encryption keys and certificates are valid. Use secure configurations and proper encryption strengths. Do not support insecure versions or configurations. This means you will continually need to check latest encryption vulnerabilities and update as needed (4.1)
- [ ] Review and implement documented best practices for encryption standards (4.1.1)
- [ ] Review and implement policies and procedures for sending/receiving credit card data (4.2.b)
- [ ] Examine system configuration and adjust encryption configuration as needed (4.1, 4.1.1)

THINGS YOU MAY NEED TO DO:

- [ ] Make sure TLS is enabled whenever cardholder data is transmitted or received through web-based services (4.1.a, 4.1.e)
- [ ] Check wireless network encryption standards (4.1.1)
- [ ] Examine keys and certificates (4.1.b)
- [ ] Review your Risk Mitigation and Migration Plan for environments that still need to use SSL and early TLS (Appendix A2.2)
- [ ] Prohibit the use of WEP, an insecure wireless encryption standard (4.1.1)

REQUIREMENT 5 IT CHECKLIST

ANTI-VIRUS UPDATES

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO DO:

- ☐ Deploy anti-virus program on commonly affected systems (5.1, 5.2)
- ☐ Protect all systems against malware and regularly update anti-virus software or programs (5.1, 5.2.b)
- ☐ Set anti-virus to detect and remove all known types of malicious software (5.1.1)
- ☐ Maintain and evaluate audit logs with IT staff (5.2.c)
- ☐ Set anti-virus to scan automatically (5.2.b)
- ☐ Make sure anti-virus system is updated automatically (definitions keep current) (5.2.a, 5.2.b)
- ☐ Make sure anti-virus cannot be disabled or altered by users (admin access only) (5.3) Document and review malware procedures and review with necessary staff (5.4)
- ☐ Examine system configurations and periodically evaluate malware threats to system (5.1.2)

REQUIREMENT 6 IT CHECKLIST

SOFTWARE UPDATES

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ Vendor supported programs, operating systems, and devices (6.2
- ☐ An update server (i.e., repository for systems to get updates)
- ☐ A change management process

THINGS YOU WILL NEED TO DO:

- ☐ Have a process in place to keep up to date with the latest identified security vulnerabilities and their threat level (6.1, 6.5.6)
- ☐ Install all vendor-supplied security patches on all system components (6.2.a)
- ☐ Ensure all security updates are installed within one month of release (6.2.b)

THINGS YOU MAY NEED TO DO:

- ☐ Set up a manual or automatic schedule to install the latest security patches for all system components

REQUIREMENT 7 IT CHECKLIST

ESTABLISH ACCESS CONTROL

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ Written policy detailing access controls for systems in the CDE (7.1, 7.3)

REQUIRED FEATURES:

- ☐ Document access control policies based on job classification and function (7.1, 7.1.1, 7.1.2, 7.1.3)
- ☐ Roles and privilege levels defined (7.1, 7.1.1)
- ☐ "Deny all" rule in place for access control systems (7.2.3)

THINGS YOU WILL NEED TO DO:

- ☐ Detail a written policy to include access to cardholder data based on job roles with privilege level, and approval/documentation of employee access (7.1, 7.1.4)
- ☐ Document policies in place with each employees' role/access and train employees on their specific access level (7.1, 7.3)

THINGS YOU MAY NEED TO DO:

- ☐ Implement access controls on any systems where cardholder data is stored and handled (7.2.1)
- ☐ Configure access controls to only allow authorized parties and deny all others without prior approval or access (7.2.2, 7.2.3)

REQUIREMENT 8 IT CHECKLIST

ID CREDENTIALS

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ Multi-factor authentication for all remote access (8.3)

THINGS YOU WILL NEED TO DO:

- ☐ Monitor all remote access accounts used by vendors, business partners, IT support personnel, etc. when the account is in use (8.1.5.b)
- ☐ Disable all remote access accounts when not in use (8.1.5.a)
- ☐ Enable accounts used for remote access only when they are needed (8.1.5.a)

THINGS YOU MAY NEED TO DO:

- ☐ Implement a multi-factor authentication solution for all remote access sessions
- ☐ Multi-factor authentication methods are as follows:
  - ☐ Something you know–password and username
  - ☐ Something you have–one-time password
  - ☐ Something you are–fingerprint or retinal scan (8.3)

REQUIREMENT 9 IT CHECKLIST

IMPROVING PHYSICAL SECURITY

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- [ ] Policies and procedures that limit the access to your physical media and devices used for processing

THINGS YOU WILL NEED TO DO:

- [ ] Restrict access to any public accessible network jacks in the business (9.1.2)
- [ ] Keep physical media secure and maintain strict control over any media being moved within the facility and outside of it (9.5, 9.5.1, 9.6.a)
- [ ] Keep electronic media in a secure area with limited access (e.g., a locked office clearly marked Management Only) and require management approval before the media is moved from its secure location (9.6.1, 9.6.3, 9.7)
- [ ] Use a secure courier when sending media through the mail so the location of the media can be tracked (9.6.2)
- [ ] Destroy media in a way that it cannot be reconstructed and if the media is separated prior to destruction, keep the media in a locked container with a clear label of "To Be Shredded" or something similar (9.8, 9.8.1)
- [ ] Maintain a list of all devices used for processing and train all employees to inspect devices for evidence of tampering. Training should include a process for verifying the identity of outside vendors wanting access to the machine, a process for reporting suspicious behavior around the machine, and a system to ensure employees know not to replace devices without management approval (9.9.2, 9.9.3)

THINGS YOU MAY NEED TO HAVE:

- [ ] A set process to train employees about proper device management and a way to report any suspicious behavior around the processing device
- [ ] A secure location to keep media, including a second secure location, if business practice is to separate media no longer needed

REQUIREMENT 10 IT CHECKLIST

LOGGING AND LOG MANAGEMENT

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ An automated audit log tracking all security-related events for all system components
- ☐ Audit logs that track:
  - ☐ Any action taken by an individual with administrative privileges (10.2.2)
  - ☐ Failed log in attempts (10.2.4)
  - ☐ Changes to accounts–including elevation of privileges, account additions, and account deletions (10.2.5)
- ☐ Identification of user, what the event type was, date and time of the event, whether the event was a success or failure, where the event originated from, and the name of affected data, system component, or resource (10.3.1-10.3.6)

THINGS YOU WILL NEED TO DO:

- ☐ Have a process in place to review the logs and security events at least daily, in addition to any reviews of system components as defined by the business for risk management strategy or other policies (10.6.1.b, 10.6.2.b)
- ☐ Have a process in place to respond to anomalies or exceptions (10.6.3.b)
- ☐ Keep all audit log records for at least one year and keep the last three months' logs readily available for analysis (10.7.b, 10.7.c)

REQUIREMENT 11 IT CHECKLIST

VULNERABILITY SCANNING & PENETRATION TESTING

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ A process for detecting and identifying wireless access points on a quarterly basis. The method should be able to identify all of the following wireless access points:
  - ☐ WLAN cards inserted into system components
  - ☐ Mobile devices used to create wireless access points (by USB or other means
  - ☐ Wireless devices attached to a network port or device (11.1.a, 11.1.b, 11.1.c)
- ☐ An inventory of authorized wireless access points with listed business justifications (11.1.1)
- ☐ A change-detection mechanism installed within the CDE to detect unauthorized modifications to critical system files, configuration files, or content files (11.5.a)

THINGS YOU WILL NEED TO DO:

- ☐ Run quarterly internal vulnerability scans using a qualified internal resource or external third party (organizational independence must exist) and re-scan all scans until high-risk (as defined in Req. 6.1) vulnerabilities are resolved (11.2.1)
- ☐ Run quarterly external vulnerability scans (requires ASV) and re-scan until all scans obtain a passing status (no vulnerability scores over 4.0) (11.2.2)
- ☐ Run internal and external scans, using a qualified resource, after any significant change to the network, and re-scan until resolved
  - ☐ For external scans – no vulnerabilities scoring 4.0 or higher exist
  - ☐ For internal scans – all high-risk vulnerabilities are resolved (11.2.3)
- ☐ Configure the change-detection mechanism to alert personnel to unauthorized modification of critical system files, configuration files, or content files; configure the tools to perform critical file comparisons at least weekly (11.5.b)
- ☐ Have a process in place to respond to alerts generated by the change-detection mechanism (11.5.1)

THINGS YOU MAY NEED TO DO:

- ☐ If wireless scanning is used to identify wireless access points, scans must be run at least quarterly (11.1.c)
- ☐ If automated monitoring is used, monitoring should generate alerts to notify personnel (11.1.d)
- ☐ Create a plan of action in the business's incident response plan for responding to the detection of unauthorized wireless access points, and take action if an unauthorized wireless access point is found (11.1.2)
- ☐ If network segmentation exists, penetration testing procedures must confirm segmentation is operational and isolates all out-of-scope systems from systems in the CDE (11.3.4.a)

REQUIREMENT 12 IT CHECKLIST

CORPORATE POLICY AND DOCUMENTATION

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ Written compliance and security policies
- ☐ Charter for PCI DSS compliance program
- ☐ Service providers must perform quarterly reviews to confirm policies and procedures are being followed.

THINGS YOU WILL NEED TO DO:

- ☐ Each employee working in the CDE must complete annual security awareness training (12.6, 12.6.1)

THINGS YOU MAY NEED TO DO:

- ☐ Create a company policy documenting all critical devices and services within the payment processing environment. Some examples include laptops, tablets, email/Internet usage, remote access, and wireless access technologies. This policy should include acceptable uses and storage of these technologies. The general purpose of this policy is to thoroughly explain each employee's role in the CDE. Review your lists annually (12.1-12.4)
- ☐ Create an approval process for allowing access to technologies and document which employees have current technology access. Keep lists readily available and review them annually (12.1-12.4)
- ☐ Create an incident response plan in the event cardholder data is compromised (12.10.1). The plan should include the following:
  - ☐ Roles and contact strategies in the event of compromise
  - ☐ Specific incident response procedures
  - ☐ Business continuity and recovery procedures Data backup processes
  - ☐ Analysis of legal requirements in reporting possible compromise Critical systems coverage and response plans
  - ☐ Notification of merchant processor and payment card brands
- ☐ Create and update a current list of third-party service providers (e.g., your IT provider, credit card machine vendor, and credit card receipt shredder).
- ☐ The following will need to be completed annually regarding your service providers (12.8, 12.8.1):
  - ☐ Establish a process for engaging with third-party providers. Best practice would be to contact them by telephone rather than taking inbound calls. Work by appointment with service providers onsite (12.8.3)
  - ☐ Obtain or update a written agreement from third-party providers acknowledging their responsibility for cardholder data they possess. Ensure they are PCI compliant themselves (12.8.2)
  - ☐ Establish a process for engaging new providers, including research prior to selecting a provider