PCI DSS 3.2 COMPLIANCE CHECKLIST

DEFEND YOUR CARDHOLDER DATA

DSS Requirement 3

Protect stored cardholder data

DO:

- □ Implement documented data retention and disposal policies to minimize cardholder data you collect and how long it is retained. (3.1)
- □ Interview your employees to confirm policies are being maintained and quarterly processes are in place to remove cardholder data outside of your retention policy. (3.1.b)
- □ Make sure the stored data and data in-transit is unreadable. (3.4, 4.1)
- □ Encrypt card data and protect the encrypted keys. (3.5)
- □ Mask your PAN data when it must be viewed using the fewest digits possible (under the 6 First, 4 Last display maximum). (3.3)
- □ Create a cardholder flow diagram for all data flows through your organization. (1.1.3)
- □ Use a data discovery tool to find misplaced sensitive data in your environment.

DON'T:

- □ Store sensitive authentication data after authorization. (3.2)
  - o **Exception:** Your organization is an issuer and has business justification.
- □ Store masked PAN data.
  - o **Solution:** Encrypt it instead.

DSS Requirement 4

Encrypt transmission of cardholder data across open, public networks

DO:

- □ Identify where you send cardholder data and ensure your policies are not violated in the journey and only trusted keys or certificates are used. (4.1)
- □ Select a sample of inbound and outbound transmissions and verify cryptography is maintained during transit. (4.1.c)

DON'T:

- □ Send PANs by end-user messaging tech like email, SMS, or IM. (4.2)
- □ Use new technologies that utilize SSL/early TLS. (version 1.0 or earlier)
- □ Migrate cardholder data to systems using SSL/early TLS. (version 1.0 or earlier)

DEFEND AGAINST THE EXTERNAL THREAT

DSS Requirement 1

Install and maintain a firewall configuration to protect cardholder data

DO:

□ Install a firewall at each internet connection (every device) an between any demilitarized zone (DMZ) and internal network zone. (1.1.4, 1.4)

□ Configure your firewalls with a description of groups responsible for network components and business justifications for all services/protocols/ports in the configuration. (1.1.5, 1.1.6)

□ Review firewall and router configuration at least every 6 months and confirm all other, non-config traffic (inbound or outbound) is denied. (1.1.7, 1.2.1)

□ Configure routers to block connections between untrusted parts of the network and cardholder data. (1.2, 1.3)

□ Assign responsibility for someone to check firewall logs daily.

DON'T:

□ Store cardholder data in the DMZ or any untrusted network.

o **Solution:** Create a secure internal network zone. (1.3.6)

DSS Requirement 2

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

DO:

- □ Identify a sys admin to be responsible for system components. (2.2.4)
- □ Maintain an inventory list of all system components in scope for PCI DSS. (2.4)
- □ Document policies to change vendor-supplied default passwords, default wireless settings and remove default accounts before installing a system on your network. (2.1, 2.1.1, 2.5)
- □ Document system component config standards that address security weaknesses, limit service/protocol access based on need, and follow hardening standards. (2.2, 2.2.2)

DON'T:

- □ Implement multiple functions to a single server as this can create permission conflicts. (2.2.1)
- □ Assume your vendors are maintaining anti-virus scanning.
    - **Requirement:** It's your responsibility to confirm vendors are up-to-date and scanning regularly.

DSS Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs

DO:

- □ Regularly update ant-virus software on your commonly affected systems and evaluate whether additional systems are at risk/ need anti-virus. (5.1, 5.1.1, 5.1.2)
- □ Automate anti-virus scans and maintain anti-virus audit logs for your systems. (5.2)
- □ Ensure only admins can alter or disable anti-virus. (5.3)
- □ Document procedures for protecting against malware. (5.4)

DON'T:

- □ Wait to identify Malware by observing the damage it causes.
    - o **Solution:** Install software that can observe behavioral anomalies and alert the necessary personnel.

DSS Requirement 6

Develop and maintain secure systems and applications

DO:

- □ Establish a process to keep up-to-date with the latest security vulnerabilities and identify the risk level. (6.1)
- □ Install all vendor-supplied security patches. (6.2.a)
- □ Document the impact, authorizer, functionality testing, and back-out procedures of all change control procedures. (6.4.5)
- □ Use strict development processes and secure coding guidelines (outlined in DSS) when developing software in-house. (6.3)

DON'T:

- □ Wait longer than 1 month to install vendor-supplied security patches for risk levels identified as critical. (6.2.b)
- □ Test in-house software in your production environment, use production data during testing, or leave test accounts/IDs after software release. (6.3.1, 6.4.1, 6.4.3)

DEFEND AGAINST THE INTERNAL THREAT

DSS Requirement 7

Restrict access to cardholder data by business need to know

DO:

□ Create a list of roles with access to the CDE that includes the definition of each role, their privilege level, and what permissions are required for each role to function. (7.1, 7.3)

□ Create a least-privilege policy for all employees and a default "deny-all" setting on all access control settings. (7.1.2, 7.2.3)

□ Require documented approval by authorizers for any privilege assignments or privilege changes in the CDE. (7.1.4)

DON'T:

□ Give excessive permissions to a role for that "rainy day" when they might require it.

o **Solution:** Use a least privilege model where permissions are granted only by business need.

o **Solution:** Grant access only for the period of time that it's needed.

DSS Requirement 8

Identify and authenticate access to system components

DO:

- □ Define and document procedures for user identification and authentication on all system components. (8.1, 8.4)
- □ Assign unique IDs to all users, test those privilege controls, and revoke access on inactive/terminated users. (8.1.1, 8.1.2, 8.1.3, 8.1.4)
- □ Monitor all accounts used by vendors and other third parties, then disable them when not in use. (8.1.5)
- □ Lock out users IDs for 30 minutes after six failed access attempts. (8.1.6, 8.1.7)
- □ Follow best practice guidelines outlined in DSS for password setting – including strong password composition, encrypting credentials, verifying ID before reset, and mandatory resets every 90 days. (8.2.1, 8.2.2, 8.2.3, 8.2.4)
- □ Incorporate multi-factor authentication for all non-console admin access and remote access to CDE. (8.3)

DON'T:

- □ Use the same password for multiple accounts or devices – once one is compromised, they all will be.
- □ Use shared user IDs or authentication methods in the CDE. (8.5)

DSS Requirement 9

Restrict physical access to cardholder data

DO: (if applicable)

□ Document process for physical access to CDE systems and a list of all devices, limiting access to roles that require it and monitoring all with authorization tokens and surveillance. (9.1.1a, 9.1.1b, 9.2, 9.3, 9.9.1)

□ Create visitor authorization and access controls that ensure visitors are identified, documented, and monitored in areas that access the CDE. (9.4)

□ Establish firm controls for physical media moved within the facility, use tracked couriers when moved outside, and ensure destroyed media cannot be reconstructed. (9.5, 9.6, 9.8)

□ Train employees with processes to identify outside vendors requesting physical access and identify/report suspicious behavior (9.9.2, 9.9.3)

DEFEND AGAINST COMPLACENCY

DSS Requirement 10

Track and monitor all access to network resources and cardholder data

DO:

- □ Implement audit trails for all systems, alerts on suspicious activity, and a response plan for those anomalies. (10.1, 10.2, 10.6.2.b)
- □ Track all admin actions, login attempts, account changes, and pauses in the audit trail. (10.2.3, 10.2.4, 10.2.5, 10.2.6)
- □ Ensure each audit log captures user ID, event type, date and time, event success or failure, where the event originated from, and what resources are affected. (10.3)
- □ Keep all audit logs for at least one year with the last three months available for analysis. (10.7)
- □ Prevent audit trail tampering and use software to alert on log changes. (10.5)
- □ Create a process that reviews CHD system logs daily, and one that reviews all other system components based on your risk assessment results. (10.6.1, 10.6.2)

DON'T:

- □ Give audit log access to anyone without a role justification. (10.5.1)
- □ Leave the daily audit trail review to manual methods – this can be a massive time void.
- □ Store audit logs for external-facing technologies on those machines – they can be compromised. (10.5.4)

DSS Requirement 11

Regularly test security systems and processes

DO:

□ Document each authorized wireless access points with a business justification. (11.1.1)

□ Implement processes to test and respond to authorized and unauthorized wireless access points on a quarterly basis. (11.1, 11.1.2)

□ Run vulnerability scans internally (with qualified personnel) and externally (with Approved Scanning Vendor) with every quarter and significant network change, correcting and re-scanning all identified vulnerabilities. (11.2)

□ Run penetration tests internally and externally (with qualified personnel or 3rd party) annually, correcting and retesting any exploitable risk found. (11.3)

□ Deploy a change-detection tool that alerts personnel to any unauthorized mod of critical systems and runs file comparisons at least weekly. (11.5)

□ Document a process for responding to change-detection alerts. (11.5.1, 11.6)

DON'T:

□ Stick to the bare-minimum for testing.

  o **Solution:** Run reviews more frequently than the bare minimum – you will respond to threats sooner, before they are exploited.

DSS Requirement 12

Maintain a policy that addresses info security for all personnel

DO:

□ Publish an annually reviewed security policy that documents all CDE critical devices and services, defines appropriate access (in role, use of that access, and location), and implements a risk assessment process. (12.1, 12.2, 12.3, 12.4)

□ Annually complete security awareness training with all personnel who access the CDE. (12.6)

□ Assign role responsibilities to document procedures, analyze security alerts, administer accounts, and monitor access to all data. (12.5)

□ Maintain documentation of service providers that requires lists of services provided, due-diligence in selection (including risk assessment), acknowledgement from SP accepting CHD responsibility, and a process to monitor the providers PCI DSS compliance. (12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5)

□ Create an annually tested response plan for a system breach that outlines tasks for each role, specific actions for different threats/alerts, how to cover critical systems and data backup, legal requirements for reporting, and notifications of card brands. (12.10)