COMPLIANCE CHECKLIST

PCI DSS

Ready for a PCI DSS Audit? While we are sure that you've already started preparing, there may still be some areas that need more attention.

REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

○ Establish and implement firewall and router configuration standards that formalize testing whenever configurations change.

○ Identify all connections between the cardholder data environment and other networks (including wireless) with documentation and diagrams.

○ Document business justification and various technical settings for each implementation.

○ Document diagram of all cardholder data flows across systems and networks.

○ Review and documents firewall rule sets at least every six months.

○ Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment.

○ Prohibit direct public access between the Internet and any system component in the cardholder data environment.

○ Install personal firewall software or equivalent functionality on any devices (including company and/or employee owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the cardholder data environment.

REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS

○ Change ALL vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.

○ Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified.

○ Using strong cryptography, encrypt all non-console administrative access.

○ Maintain an inventory of system components that are in scope for PCI DSS.

○ Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

○ Those who are shared hosting providers must protect each entity's hosted environment and cardholder data

REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA

○ Document your data retention policy for cardholder data storage and retention time to that which is required for business, legal, and/or regulatory purposes.

○ Securely delete unnecessary stored data at least quarterly.

○ Do not store sensitive authentication data after authorization (even if it is encrypted).

○ Render all sensitive authentication data unrecoverable upon completion of the authorization process. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely.

○ Mask PAN when displayed (the first six and last four digits are the maximum number of digits you may display), so that only authorized people with a legitimate business need can see more than the first six/last four digits of the PAN.

○ Render PAN unreadable anywhere it is stored (e.g. portable digital media, backup media, in logs, and data received from or stored by wireless networks). Use strong one-way hash functions of the entire PAN, truncation, index tokens with securely stored pads, or strong cryptography for protecting PAN.

○ Document and implement procedures to protect any keys used for encryption of cardholder data from disclosure and misuse.

○ Fully document and implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.

REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS

○ Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, cellular technologies, GPRS, satellite communications).

○ Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong encryption for authentication and transmission.

○ Do not send unprotected PANs by end user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).

REQUIREMENT 5: PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

○ Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

○ Systems not affected commonly by malicious software, perform periodic evaluations to evaluate evolving malware threats and confirm whether such systems continue to not require anti-virus software.

○ Ensure that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs, which are retained per PCI DSS Requirement 10.7.

○ Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

○ Establish a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

○ Protect all system components and software from known vulnerabilities by installing applicable vendor- supplied security patches.

○ Install critical security patches within one month of release.

○ Develop internal and external software applications including web-based administrative access to applications in accordance with PCI DSS and based on industry best practices.

○ Incorporate information security throughout the software development life cycle. This applies to all software developed internally as well as bespoke or custom software developed by a third party.

○ Follow change control processes and procedures for all changes to system components. All relevant PCI DSS requirements must be implemented on new or changed systems and networks after significant changes.

○ Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and developing applications based on secure coding guidelines – including how sensitive data is handled in memory.

○ Ensure all public-facing web applications are protected against known attacks, either by performing application vulnerability assessment at least annually and after any changes, or by installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

REQUIREMENT 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED- TO-KNOW

○ Restrict access to system components and cardholder data to only those individuals whose job requires such access.

○ Establish an access control system(s) for systems components that restricts access based on a user's need to know basis and is set to "deny all" unless specifically allowed.

REQUIREMENT 8: IDENTIFY AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS

○ Assign all users a unique username before allowing them to access system components or cardholder data.

○ Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric.

○ Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography.

○ Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication. This requirement applies to administrative personnel with non-console access to the CDE from within the entity's network, and all remote network access (including for users, administrators, and third parties) originating from outside the entity's network.

○ Do not use group, shared, or generic IDs, or other authentication methods. Service providers with access to customer environments must use a unique authentication credential (such as a password/passphrase) for each customer environment.

○ Physical security tokens, smart cards, and client-side certificates must be assigned to an individual account.

○ All access to any database containing cardholder data must be restricted: all user access must be through programmatic methods; only database administrators can have direct or query access; and application IDs for database applications can only be used by the applications (and not by users or non-application processes).

REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

- ○ Limit and monitor physical access to systems in the cardholder data environment by implementing CCTV/Physical access control system.
- ○ Implement procedures to easily distinguish between onsite personnel and visitors, such as assigning ID badges.
- ○ Restrict physical access for onsite personnel to the sensitive areas based authorized individuals and based on individual job function.
- ○ Access must be revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc. returned or disabled.
- ○ Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained, given a physical badge or other identification that expires and identifies visitors as not onsite personnel, and are asked to surrender the physical badge before leaving the facility or at the date of expiration.
- ○ Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name, company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law.
- ○ Physically secure all media.
- ○ Store media back-ups in a secure location, preferably off site.
- ○ Maintain strict control over the internal or external distribution of any kind of media.
- ○ Maintain strict control over the storage and accessibility of media.
- ○ Destroy media when it is no longer needed for business or legal reasons.
- ○ Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. This includes periodic inspections of POS device surfaces to detect tampering, and training personnel to be aware of suspicious activity.

REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

- ○ Implement automated audit trails to link all access to system components to each individual user for reconstructing these events:
  - ○ All individual user accesses to cardholder data
  - ○ All actions taken by any individual with root or administrative privileges
  - ○ Access to all audit trails
  - ○ Invalid logical access attempts
  - ○ Use of and changes to identification and authentication mechanisms
  - ○ All changes, additions, deletions to accounts with root or administrative privileges
  - ○ Initialization, stopping or pausing of the audit logs
  - ○ Creation and deletion of system-level objects
- ○ Audit trail entries for all system components for each event must record at a minimum
  - ○ User identification
  - ○ Type of event
  - ○ Date and time
  - ○ Success or failure indication
  - ○ Origination of event
  - ○ Identity or name of affected data, system component or resource

- ○ Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.
- ○ Secure audit trails so they cannot be altered.
- ○ Review logs and security events for all system components to identify anomalies or suspicious activity.
- ○ Perform critical log reviews at least daily.
- ○ Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.
- ○ Service providers must implement a process for timely detection and reporting of failures of critical security control systems.

REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

- ○ Detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
- ○ Maintain an inventory of authorized wireless access points and implement incident response procedures in the event unauthorized wireless access points are detected.
- ○ Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.
- ○ Address vulnerabilities and perform rescans as needed, until passing scans are achieved.
- ○ Create and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification.
- ○ If segmentation is used to reduce PCI DSS scope, perform penetration tests (at least annually for non- service providers and least six months for service providers) to verify the segmentation methods are operational and effective.
- ○ Implement network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.
- ○ Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files.
- ○ Configure the software to perform critical file comparisons at least weekly.

REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR ALL PERSONNEL

○ Establish, publish, maintain, and disseminate a security policy; review the security policy at least annually and update when the environment changes.

○ Implement a risk assessment process that is performed at least annually and upon significant changes to the environment that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment.

○ Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.

○ Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. Service providers must also establish responsibility for their executive management for the protection of cardholder data and a PCI DSS compliance program.

○ Assign to an individual or team information security responsibilities defined by 12.5 subsections.

○ Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

○ Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Example screening includes previous employment history, criminal record, credit history, and reference checks.

○ Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.

○ Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data that they possess or otherwise store, process, or transmit on behalf of the customer, or to the extent they could impact the security of the customer's cardholder data environment.

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

○ Service providers must perform and document reviews at least quarterly to confirm personnel are following security policies and operational procedures.

○ Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

ABOUT CONTROLCASE

ControlCase is a global provider of certification, cybersecurity and continuous compliance services. ControlCase is committed to empowering organizations to develop and deploy strategic information security and compliance programs that are simplified, cost effective, and comprehensive in both on-premise and cloud environments. ControlCase offers certifications and a broad spectrum of cybersecurity services that meet the needs of companies required to certify to PCI DSS, HITRUST, SOC 2 Type II, ISO 27001, PCI PIN, PCI P2PE, PCI TSP, PCI SSF, CSA STAR, HIPAA, GDPR, SWIFT, and FedRAMP.

ControlCase

www.controlcase.com

USA & Canada: **+1-703-483-6383** | India: **+91-22-50323006**

12015 Lee Jackson Memorial Hwy, Suite 520, Fairfax, VA 22033