# Credit and Debit Card Handling Policy

## Purpose

This Policy outlines Alight’s framework for the proper handling of cardholder data processed through automated systems and/or manual procedures.

Alight recognizes the value of accepting credit and debit cards as payment for goods and services. This Policy provides guidance to ensure handling of cardholder data aligns with Alight’s program to comply with Payment Card Industry Data Security Standards (PCI DSS).

## Scope

The scope of this Policy is global, which includes all business units, all regions, and all entities of Hewitt Associates plc (“Alight”) that obtain, process, store and/or transmit cardholder data as a merchant and/or service provider. Alight refers to all wholly-owned subsidiaries of Hewitt Associates plc, all subsidiaries in which Hewitt Associates plc has a controlling interest, and all agents or authorized representatives of Hewitt Associates plc or its subsidiaries.

## Applicable Audience

This Policy applies to all colleagues and contractors of Alight that come in contact with cardholder data. The term "colleague" refers to all full-time employees, part-time employees, temporary employees, and interns who provide services to Alight. The term “contractor” refers to any individual on another company’s payroll (contactors, outsourcers, consultants, contingent workers, temporary agency workers, etc.) who provides services to Alight.

## Rationale

As credit and debit card acceptance and electronic commerce continue to grow, the card companies (e.g. VISA, MasterCard) have established requirements in order to protect cardholder data. The requirements are referred to as the Payment Card Industry Data Security Standard or PCI DSS. Any organization that handles cardholder data must be compliant with PCI DSS and certify their compliance on an annual basis. Not complying with PCI DSS could lead to fines from card brands, issuers and/or merchant banks and potentially revoke Alight’s ability to process payment via credit / debit card.

## Compliance & Enforcement

Compliance with this Policy is mandatory.

Potential violations of this policy are subject to review and investigation by Alight and/or its agents. Violations of this policy may result in discipline, up to and including removal of assignment, end of contract for vendors, or termination. This is subject to the procedural requirements of the countries in which Alight operates. Alight reserves the right to refer for prosecution any violations of this policy. Violations of this policy may also result in fines from merchants, acquiring banks, and/or clients.

Alight reserves the right to modify the Policy at its sole discretion.

## Definitions

**PCI:** Payment Card Industry

**PCI DSS:** Payment Card Industry Data Security Standards

**PCI SSC:** Payment Card Industry Security Standards Council. An open global forum launched in 2006 that is responsible for the development, management, education, and awareness of the PCI Security Standards. The council is made up of the five global payment brands (America Express, Discover, VISA, JBC, MasterCard)

**Merchant:** A business unit or 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

**Service Provider:** A business storing, processing or transmitting cardholder data on behalf of other merchants or service providers

**Cardholder Data:** Cardholder Data represents any personal information of the cardholder. This could be the Primary Account Number (PAN), expiration date, name, Card Verification Code (CVC), or any other cardholder’s identifying information (refer to figures 1.1 and 1.2 below)

Figure 1.1

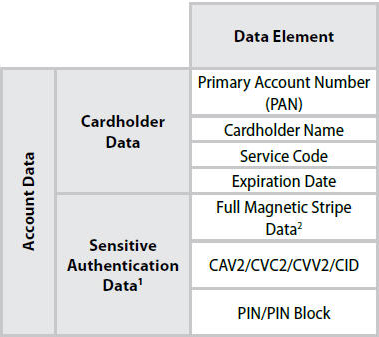
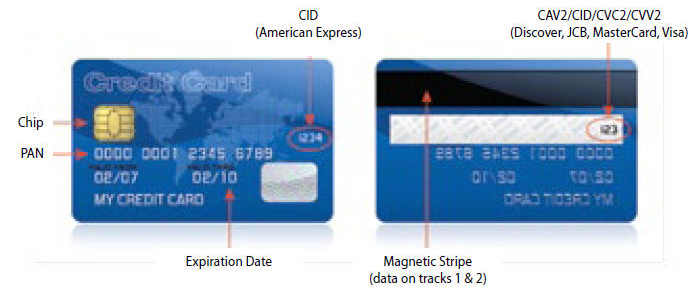


Figure 1.2



Note – PCI DSS only applies if PAN is obtained, stored, processed and/or transmitted

**Cardholder Data Environment:** System components used to obtain, process, store or transmit cardholder data, and any other component that resides on the same network segment as those system components

**Network Segmentation:** System handling cardholder data is isolated / segmented from rest of the network, therefore placing the rest of that network outside the scope of the assessment. Network segmentation could be achieved using firewall, routers and/or VLANs

**Merchant / Acquiring Bank:** Bank or entity the merchant uses to process their payment card transactions. Once the transactions are processed the funds are deposited into the merchant banks account

**Self-Assessment Questionnaire (SAQ):** The SAQ is a validation tool introduced by card brands and required by merchant banks for merchants to self-assess against the PCI DSS controls. There are multiple types of SAQ based on how the cardholder data is handled

**Qualified Security Assessor (QSA):** Approved by PCI council, QSA provides guidance and conducts the PCI DSS assessment on behalf of the merchant or service provider

**In-house:** Cardholder data being handled by Alight managed systems or Alight personnel. These systems could be hosted within an Alight controlled data center or at a 3rd party hosting provider, such as managed hosting provider

**Virtual Terminal:** A web-browser based terminal connecting to acquirer, card processor or third party service provider website to authorize payment card transactions, where merchant manually enters cardholder data via securely connected web browser

**POS Terminal:** Point of Sale terminal to process “card not present” and “card present” transactions. Cardholder data is manually entered or physically swiped on the POS terminal for processing

## Policy Statements

### Industry Requirements

#### Control Requirements

PCI DSS requires adherence to all of GSS Security Policies & Procedures posted on Alight’s Colleague Portal.

In addition to GSS policies and procedures, implementation of the requirements below are required. Any requirements marked as “N/A” – must be reviewed by GSS to ensure appropriate justification exists for limiting assessment responses

1. Install and maintain a firewall configuration to protect cardholder data
   * 1. Maintain network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks
     2. Maintain diagram that shows all cardholder data flows across systems and networks
     3. Ensure a firewall exists at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
     4. Maintain a description of groups, roles, and responsibilities for management of network components

1.1.6 Document business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

1.1.7 Review firewall and router rule sets at least every six months

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

1.2.2 Secure and synchronize router configuration files.

1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

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

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.

1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.

1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)

1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

1.3.5 Permit only “established” connections into the network.

1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.

1.4 Install personal firewall software or equivalent functionality on any portable computing 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 CDE. Firewall (or equivalent) configurations include:

* Specific configuration settings are defined.
* Personal firewall (or equivalent functionality) is actively running.
* Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.

1. Do not use vendor-supplied defaults for system passwords and other security parameter
   1. For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
   2. Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.
   3. Enable only necessary services, protocols, daemons, etc., as required for the function of the system.
   4. Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
   5. Configure system security parameters to prevent misuse.
   6. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
   7. Encrypt all non-console administrative access using strong cryptography. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.
      1. Maintain an inventory of system components that are in scope for PCI DSS.
      2. Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
      3. Shared hosting providers supporting the cardholder environment must protect each entity’s hosted environment and cardholder data.
2. Protect stored cardholder data

3.1.0 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

* Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements
* Processes for secure deletion of data when no longer needed
* Specific retention requirements for cardholder data

3.2.0 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:

3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:

* The cardholder’s name
* Primary account number (PAN)
* Expiration date
* Service code to minimize risk, store only these data elements as needed for business.

3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

* One-way hashes based on strong cryptography, (hash must be of the entire PAN)
* Truncation (hashing cannot be used to replace the truncated segment of PAN)
* Index tokens and pads (pads must be securely stored)
* Strong cryptography with associated key-management processes and procedures.

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.

3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:

* Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key
* Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device)
* As at least two full-length key components or key shares, in accordance with an industry-accepted method

3.5.4 Store cryptographic keys in the fewest possible locations.

3.6.0 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:

3.6.1 Generation of strong cryptographic keys

3.6.2 Secure cryptographic key distribution.

3.6.3 Secure cryptographic key storage

3.6.4 Cryptographic key changes for keys that have reached the end of their crypto period (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.

3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.

3.6.7 Prevention of unauthorized substitution of cryptographic keys.

3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

1. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:

* Only trusted keys and certificates are accepted.
* The protocol in use only supports secure versions or configurations.
* The encryption strength is appropriate for the encryption methodology in use.

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control is prohibited.

4.2.0 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).

4.3.0 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.

1. User and regularly update anti-virus software or programs

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

5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

5.2.0 Ensure that all anti-virus mechanisms are maintained as follows:

* Are kept current
* Perform periodic scans
* Generate audit logs which are retained per PCI DSS Requirement 10.7.

5.3.0 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.

5.4.0 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.

1. Develop and maintain secure systems and applications

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.

6.3.0 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:

* In accordance with PCI DSS (for example, secure authentication and logging)
* Based on industry standards and/or best practices.
* Incorporating information security throughout the software-development life cycle

6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.

6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:

* Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.
* Code reviews ensure code is developed according to secure coding guidelines
* Appropriate corrections are implemented prior to release.
* Code-review results are reviewed and approved by management prior to release.

6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.

6.4.2 Separation of duties between development/test and production environments

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

6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.

6.4.5 Change control procedures must include the following:

6.4.5.1 Documentation of impact.

6.4.5.2 Documented change approval by authorized parties.

6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.

6.4.5.4 Back-out procedures.

6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

6.5.2 Buffer overflow

6.5.3 Insecure cryptographic storage

6.5.4 Insecure communications

6.5.5 Improper error handling

6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).

6.5.7 Cross-site scripting (XSS)

6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).

6.5.9 Cross-site request forgery (CSRF)

6.5.10 Broken authentication and session management

6.6.0 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

* Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.
* 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.

1. Restrict access to cardholder data by business need-to-know

7.1.0 Limit access to system components and cardholder data to only those individuals whose job requires such access.

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

7.1.3 Assign access based on individual personnel’s job classification and function.

7.1.4 Require documented approval by authorized parties specifying required privileges.

7.2 Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.

7.2.1 Implement access control systems on all system components.

7.2.3 Confirm that the access control systems have a default “deny-all” setting.

1. Identify and authenticate access to system components

8.1.3 Immediately revoke access for any terminated users.

8.1.4 Remove/disable inactive user accounts at least every 90 days.

8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:

* Enabled only during the time period needed and disabled when not in use.
* Monitor when in use.

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

8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

8.2.0 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:

* 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.

8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.

8.2.3 Passwords/passphrases must meet the following:

* Require a minimum length of at least seven characters.
* Contain both numeric and alphabetic characters.

Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.

8.2.4 Change user passwords/passphrases at least every 90 days.

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

8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity’s network.

8.5.0 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

* Generic user IDs are disabled or removed.
* Shared user IDs do not exist for system administration and other critical functions.
* Shared and generic user IDs are not used to administer any system components.

8.5.1 Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

8.6.0 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:

* Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
* Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

8.7.0 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

* All user access to, user queries of, and user actions on databases are through programmatic methods.
* Only database administrators have the ability to directly access or query databases.
* Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

1. Restrict physical access to cardholder data

9.1.0 Limit and monitor physical access to systems in the cardholder data environment.

9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.

9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks.

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

9.2.0 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.

9.3.0 Control physical access for onsite personnel to the sensitive areas as follows:

* Access must be authorized and based on individual job function.
* Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

9.4.1 Visitors must be authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.

9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.

9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.

9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.

9.5.0 Physically secure all media.

9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location’s security at least annually.

9.6.0 Maintain strict control over the internal or external distribution of any kind of media, including the following:

9.6.1 Classify media so the sensitivity of the data can be determined.

9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.

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

9.7.0 Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.

9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.

9.8.0 Destroy media when it is no longer needed for business or legal reasons as follows:

9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.

9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

9.0 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

9.1 Maintain an up-to-date list of devices. The list should include the following:

* Make, model of device
* Location of device (for example, the address of the site or facility where the device is located)
* Device serial number or other method of unique identification.

9.9.2 Periodically inspect device surfaces to detect tampering

9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:

* Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
* Do not install, replace, or return devices without verification.
* Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
* Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

10 Track and monitor all access to network resources and cardholder data

10.1.0 Implement audit trails to link all access to system components to each individual user.

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

10.2.1 All individual user accesses to cardholder data

10.2.2 All actions taken by any individual with root or administrative privileges

10.2.3 Access to all audit trails

10.2.4 Invalid logical access attempts

10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges

10.2.6 Initialization, stopping, or pausing of the audit logs

Creation and deletion of system-level objects

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

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and Time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource

10.4.0 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).

10.4.1 Critical systems have the correct and consistent time.

10.4.2 Time data is protected.

10.4.3 Time settings are received from industry-accepted time sources.

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

10.5.2 Protect audit trail files from unauthorized modifications.

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

10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.

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

10.6.1 Review the following at least daily:

* All security events
* Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
* Logs of all critical system components
* Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

10.6.2 Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment.

10.6.3 Follow up exceptions and anomalies identified during the review process.

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).

10.8 Implement a process for the timely detection and reporting of failures of critical security control systems

10.8.1 Respond to failures of any critical security controls in a timely manner.

10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.

1. Regularly test security systems and processes

11.1 Test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.

11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.

11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.

11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.

11.2.4 System configuration standards must be updated as new vulnerability issues are identified.

11.2.5 All new system implementations must have configuration standards applied and verified as being in place prior to be placed in production

11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification

11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification

11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

11.3.4.1 Confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.

11.3.5 For PCI systems, the business must utilize an Alight-approved third party provider to conduct required penetration testing. Third parties leveraged for this service must demonstrate adherence to the requirements as specified by PCI DSS prior to engagement. The third party must:

* Demonstrate an industry-accepted approach (for example: NIST SP800-115)
* Demonstrate industry standard certification (for example OSCP, CEH, etc.)
* Include coverage for the full CDE perimeter and critical systems
* Include testing from inside and outside the network
* include, at a minimum, the following vulnerabilities: Injection flaws, Buffer overflow, Insecure cryptographic storage, Insecure communications, Improper error handling, All “high risk” vulnerabilities identified in the vulnerability identification process, Cross-site scripting, Improper access control, Cross-site request forgery, Broken authentication and session management
* Include network layer penetration tests to include components that support network function and operating systems
* Include and consider threats and vulnerabilities experienced in the last 12 months
* Provide Alight with the final report to include in the PCI assessment package
* If cardholder data is obtained during penetration testing this must not be stored by the third party and should be purged following the delivery of final report
* Findings must be remediated to address any exploitable vulnerability. A retest to validate newly implemented controls must be conducted following remediation. This could require a new engagement

11.4 Use 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 in the cardholder data environment, and alert personnel to suspected compromises.

11.5 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; and configure the software to perform critical file comparisons at least weekly.

11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.

11.6.0 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.

1. Maintain a policy that addresses information security for all personnel.

12.1 Establish, publish, maintain, and disseminate a security policy.

12.1.1 Review the security policy at least annually and update the policy when the environment changes.

12.2 Implement a risk-assessment process

12.3.1 Critical technologies in the cardholder environment require explicit approval by authorized parties

12.3.2 Critical technologies in the cardholder environment require authentication for use of the technology

12.3.3 A list of all devices and personnel with access to technology in the card holder environment must be maintained

12.3.4 Owner, contact information, and purpose for all critical technology in the cardholder environment must be maintained

12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity

12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use

12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.

Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:

* Overall accountability for maintaining PCI DSS compliance
* Defining a charter for a PCI DSS compliance program and communication to executive management

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

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

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

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

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

12.5.5 Monitor and control all access to data.

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

12.6.1 Educate personnel upon hire and at least annually.

12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.

12.7.0 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)

12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

12.8.1 Maintain a list of service providers including a description of the service provided.

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.

12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

12.8.4 Maintain a program to monitor service providers’ PCI DSS compliance status at least annually.

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

12.9.0 Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.

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

12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

* Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum
* Specific incident response procedures
* Business recovery and continuity procedures
* Data backup processes
* Analysis of legal requirements for reporting compromises
* Coverage and responses of all critical system components
* Reference or inclusion of incident response procedures from the payment brands."

12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.

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

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

12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.

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

12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:

* Daily log reviews
* Firewall rule-set reviews
* Applying configuration standards to new systems
* Responding to security alerts
* Change management processes

12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include:

* Documenting results of the reviews
* Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program

### Validation Requirements

* 1. Annual completion of the applicable SAQ or ROC assessment against environment containing the cardholder data
     + Merchant
       1. Conduct self-assessment if annual transaction volume is < 6,000,000. A PCI DSS QSA can be used if internal expertise does not exist to assess the environment
       2. Assessment must be completed by PCI DSS QSA if transaction volume is > 6,000,000 or considered a level 1 by the acquirer or merchant bank
     + Service Provider
     + Conduct self-assessment if annual transaction volume is < 300,000. A PCI DSS QSA can be used if internal expertise does not exist to assess the environment
     + Assessment must be completed by PCI DSS QSA if transaction volume is > 300,000
  2. External and internal PCI DSS scanning of web facing system handling cardholder data
  3. Results of SAQ must be submitted annually and results of external scan must be submitted to the merchant banks as defined by banks as required

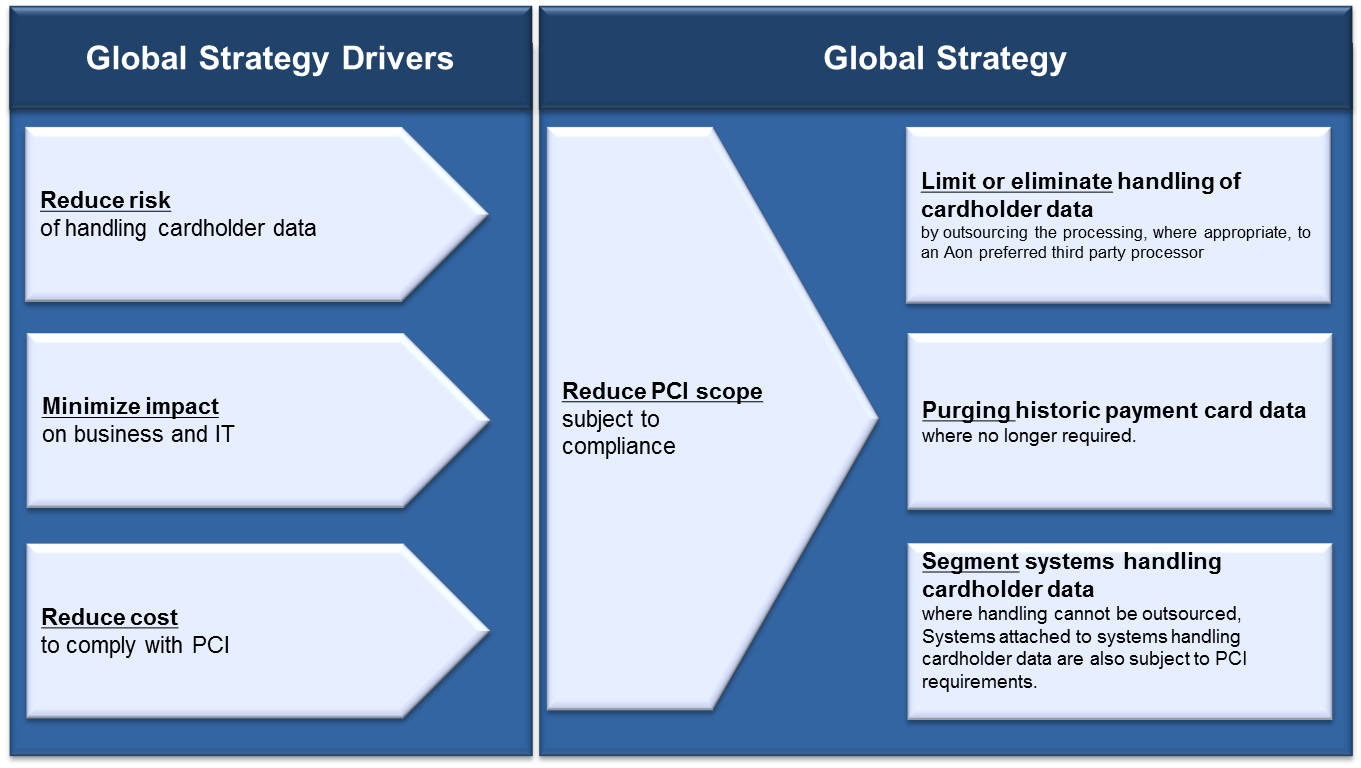
### Alight’s Requirements

### Roles and Responsibilities

* 1. Global Security Services (GSS)
     1. Develop and maintain PCI DSS strategy and documentation
     2. Define validation requirements and provide PCI guidance to Alight business
     3. Provide oversight for completion of SAQ or ROC
     4. Keep Alight executives and external parties informed of Alight’s PCI DSS status globally
     5. Develop framework and program for on-going compliance
  2. Global Security Services
     + 1. Perform PCI DSS vulnerability scan (i.e. 2.2)
  3. Business Unit(s) handling cardholder data
     1. Review and understand PCI DSS and associated risk
     2. Assign single point of contact (BU PCI lead) to interface with GSS and manage execution of PCI strategy
     3. If a service provider is used, document roles and responsibilities of the service provider and PCI DSS control ownership for Alight and service provider and ensure they are PCI DSS compliant
     4. Engage GSS during the selection process of a new service provider supporting the cardholder environment
     5. Understand and conduct the compliance validation requirements
     6. Maintain ongoing compliance
     7. Review and update Network Diagrams and Data Flow diagrams at least annually and/or after a change to the Card Data Environment
     8. Complete annual SAQ and remediate issues as required
     9. QSA assessment (if QSA assessment required) and associated costs
     10. PCI gap remediation identified in the SAQ and associated costs
     11. Inform Global Security Services(GSS) of any business or IT changes with potential to impact the cardholder environment or scope

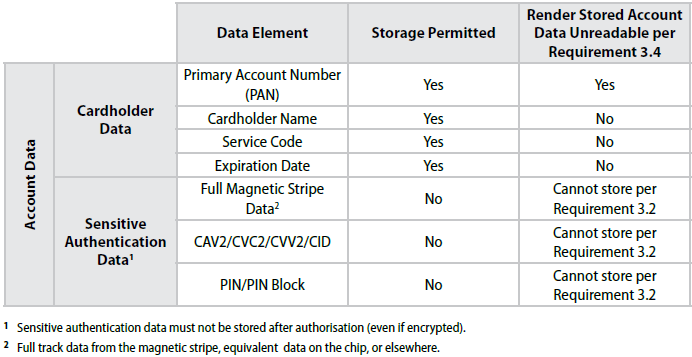
### Alight’s Strategy to Comply with PCI DSS

* 1. Mitigate the risk of handling cardholder data and significant cost of compliance by transferring that risk to a PCI DSS compliant third party card processor



### Approved In-House Methods for Handling Cardholder Data

* 1. In-house handling of cardholder data requires valid business rationale along with approval from BU CFO, GSS and business unit PCI lead
  2. Obtaining cardholder data
     1. Cardholder data should only be obtained using secure website, standalone fax machine, post mail, telephone calls, or in person
     2. All applicable PCI DSS controls must be maintained and assessed
  3. Transmitting cardholder data
     1. If cardholder data is transmitted over public internet, it must be encrypted
     2. eCommerce sites that transmit cardholder data must be segmented from non-cardholder data environment and cannot store cardholder data at rest
     3. All applicable PCI DSS controls must be maintained and assessed
  4. Storing cardholder data in electronic format



* + 1. Storage of cardholder data is prohibited. Exceptions can only be made if the storage methods are compliant with PCI DSS, legal and contractual obligations. Approval for exceptions must be obtained from GSS.
    2. Systems storing cardholder data must be segmented from non-cardholder data environments
    3. CVV code along with the full PAN number must never be stored post authorization even in encrypted format
    4. Quarterly PCI DSS vulnerability scan must be completed and all critical and high vulnerability must be remediated
  1. Storing cardholder data in paper format
     1. Paper records containing cardholder data must be secured and accessible only to authorized personnel
     2. All applicable PCI DSS controls must be maintained and assessed
  2. Processing cardholder data
     1. A POS terminal being used to process cardholder data must be PCI DSS compliant
     2. A company desktop or laptop being used as a virtual terminal to process cardholder data must have a personal firewall installed and configured
     3. All applicable PCI DSS controls must be maintained and assessed
  3. Note – this policy only covers PCI requirements and is not to be used in lieu of Alight’s Information Security Policies except where PCI requirements are more stringent

1. Requirements for Service Providers
   1. Service providers processing cardholder data on behalf of Alight or supporting infrastructure / application that is handling cardholder data must be compliant with PCI DSS applicable controls
   2. PCI DSS control ownership matrix must be completed to document who is responsible for executing the control and producing evidence
   3. Service providers must provide Attestation of Compliance (AOC) or Report on Compliance document showing compliance with applicable PCI DSS requirements
   4. Contract between Alight and service providers must include an acknowledgement that the service provider is responsible for the security of the cardholder data

## Reference Documents

[PCI DSS v3.2](https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss)

[PCI DSS FAQ](https://www.pcisecuritystandards.org/faq/)

Alight Security Policies and Standards

[PCI DSS Council home page](https://www.pcisecuritystandards.org/)

[Copy of SAQ and other reference documents](https://www.pcisecuritystandards.org/security_standards/documents.php)

## Reporting a Data Breach

All data security / privacy incidents including potential compromise of card holder data should be reported to the Alight Global Emergency Operations Center at +1-866-730-1442 (Americas) or +443-569-8235 (International) or via email to [global.eoc.mailbox@aon.com](mailto:global.eoc.mailbox@aon.com).

## Legal Conflicts

Alight’s Security Policies and Standards were drafted to address the protections found in existing laws and regulations and may be amended as necessary due to law, regulation, or business requirements. There is no intent to conflict with relevant laws or regulations. In the event of any conflict with relevant laws or regulations, they will control.

Alight’s Security Policies and Standards may be supplemented by other policies or standards of Alight. In the case of a conflict or ambiguity, the more specific provisions of any such policy or standard of Alight shall take precedence over the more general provisions contained in Alight Security Policies and Standards.

## Exceptions

Exceptional circumstances occur from time to time. In these situations, contact your regional PCI DSS lead.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
|  |  |
| Primary Contact | Alight Global Security Services | [global.security.services@Aon.com](mailto:global.security.services@Aon.com) |
| Version Number | 2.4 |
| Owner | Alight Global Security Services | Risk Controls and Assessments |
| Author(s) | Alight Global Security Services | Risk Controls and Assessments |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | September 18, 2015 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2014 August | Original | No standards added or moved. Minor updates to some wording for clarification purposes only. |
| 2.0 | 2015 August | Minor Updates | No standards added or moved. Minor updates to some wording for clarification purposes only. |
| 2.1 | 2016 July | 2016 Policy Review | No standards added or moved. Minor updates to organizational changes only |
| 2.2 | 2016 October | Minor Update | Minor Update to 1.12 – add comment to review list PCI DSS v3.2 template for Report on Compliance for a list of all requirements. |
| 2.3 | 2016 November | Update | Update for expansion of PCI DSS requirements |
| 2.4 | 2017 January | Update | Added wording 11.2.4, 11.2.5 and 11.3.5 |
| 2.5 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |