Responsibility Matrix for Clients who utilize 1800 Notify Payment Solutions

PCI DSS 4.0

This also will be used to satisfy PCI DSS requirement 12.8 related to MSP's.

Questions?
Contact: info@1800notify.com
Subject: PCI DSS 4.0 Responsbility Matrix
Attn: Chief Information Security Officer

Build and Maintain a Secure Network and Systems							
Payment Card Information (PCI) DSS Requirements	Guidance	Control Ownership			Implementation Details		
		1800	Client	Shared	1800 Notify	Client
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Network security controls (NSCs), examine all network traffic entering (ingress) and leaving (egress) a segment and decide, based on the policies defined, whether the network traffic is allowed to pass or whether it should be rejected. Typically, NSCs are placed between environments with different security needs or levels of trust, however in some environments NSCs control the traffic to individual devices irrespective of trust boundaries. Policy enforcement generally occurs at layer 3 of the OSI model, but data present in higher layers is also frequently used to determine policy decisions.	X				
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. **Customized Approach Objective** Expectations, controls, and oversight for meeting activities within Requirement 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Requirement 1.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 1. While it is important to define the specific policies or procedures called out in Requirement 1, it is equally important to ensure they are properly documented, maintained, and disseminated. It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For these reasons, consider updating these documents as soon as possible after a change			X	1800 Notify matains security policies and operational procedures that are compliant with PCI DSS	The client must also matain security policies and operational procedures that are compliant with PCI DSS
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood. **Customized Approach Objective** Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.	X				
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained. **Customized Approach Objective** The way that NSCs are configured and operate are defined and consistently applied.	These standards often define the requirements for acceptable protocols, ports that are permitted to be used, and specific configuration requirements that are acceptable. Configuration standards may also outline what the entity considers not acceptable or not permitted within its network.	X				
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1. **Customized Approach Objective**	Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Verification should provide reasonable assurance that the change did not adversely impact the security of the network and that the change performs as expected.	X				
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks. **Customized Approach Objective**	Maintaining an accurate and up-to-date network diagram(s) prevents network connections and devices from being overlooked and unknowingly left unsecured and vulnerable to compromise. A properly maintained network diagram(s) helps an organization verify its PCI DSS scope by identifying systems connecting to and from the CDE.	X				
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment. **Customized Approach Objective**	An up-to-date, readily available data-flow diagram helps an organization understand and keep track of the scope of its environment by showing how account data flows across networks and between individual systems and devices. Maintaining an up-to-date data-flow diagram(s) prevents account data from being overlooked and unknowingly left unsecured.	X				
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need. **Customized Approach Objective**	The security risk associated with each service, protocol, and port allowed should be understood. Approvals should be granted by personnel independent of those managing the configuration. Approving personnel should possess knowledge and accountability appropriate for making approval decisions.	X				

1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated. **Customized Approach Objective**	If insecure services, protocols, or ports are necessary for business, the risk posed by these services, protocols, and ports should be clearly understood and accepted by the organization, the use of the service, protocol, or port should be justified, and the security features that mitigate the risk of using these services, protocols, and ports should be defined and implemented by the entity.	X				
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective. **Customized Approach Objective**	Such a review gives the organization an opportunity to clean up any unneeded, outdated, or incorrect rules and configurations which could be utilized by an unauthorized person. Furthermore, it ensures that all rules and configurations allow only authorized services, protocols, and ports that match the documented business justifications.	X				
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations. **Customized Approach Objective** NSCs cannot be defined or modified using untrusted configuration objects (including files).	To prevent unauthorized configurations from being applied to the network, stored files with configurations for network controls need to be kept up to date and secured against unauthorized changes. Keeping configuration information current and secure ensures that the correct settings for NSCs are applied whenever the configuration is run. Examples If the secure configuration for a router is stored in non-volatile memory, when that router is restarted or rebooted, these controls should ensure that its secure configuration is reinstated.	X				
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied. **Customized Approach Objective** Unauthorized traffic cannot enter the CDE.	All traffic inbound to the CDE, regardless of where it originates, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to ensure traffic is restricted to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content.	X				
1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied. **Customized Approach Objective** Unauthorized traffic cannot leave the CDE.	All traffic outbound from the CDE, regardless of the destination, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content.	X				
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE. **Customized Approach Objective**	The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and account data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If NSCs do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information.	X				
1.4.1 NSCs are implemented between trusted and untrusted networks. **Customized Approach Objective**	An entity could implement a DMZ, which is a part of the network that manages connections between an untrusted network (for examples of untrusted networks refer to the Requirement 1 Overview) and services that an organization needs to have available to the public, such as a web server. Please note that if an entity's DMZ processes or transmits account data (for example, e-commerce website), it is also considered a CDE.	X				

1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied. **Customized Approach Objective** Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.	Ensuring that public access to a system component is specifically authorized reduces the risk of system components being unnecessarily exposed to untrusted networks. Maintaining the "state" (or status) for each connection into a network means the NSC "knows" whether an apparent response to a previous connection is a valid, authorized response (since the NSC retains each connection's status) or whether it is malicious traffic trying to fool the NSC into allowing the connection.	X				
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network. **Customized Approach Objective** Packets with forged IP source addresses cannot enter a trusted network.	Filtering packets coming into the trusted network helps to, among other things, ensure packets are not "spoofed" to appear as if they are coming from an organization's own internal network. For example, anti-spoofing measures prevent internal addresses originating from the Internet from passing into the DMZ.	X				
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks. **Customized Approach Objective** Stored cardholder data cannot be accessed from untrusted networks.	Cardholder data that is directly accessible from an untrusted network, for example, because it is stored on a system within the DMZ or in a cloud database service, is easier for an external attacker to access because there are fewer defensive layers to penetrate. Using NSCs to ensure that system components that store cardholder data (such as a database or a file) can only be directly accessed from trusted networks can prevent unauthorized network traffic from reaching the system component.	X				
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties. **Customized Approach Objective** Internal network information is protected from unauthorized disclosure.	Restricting the disclosure of internal, private, and local IP addresses is useful to prevent a hacker from obtaining knowledge of these IP addresses and using that information to access the network. Methods used to meet the intent of this requirement may vary, depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.	X				
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. **Customized Approach Objective**	Computing devices that are allowed to connect to the Internet from outside the corporate environment—for example, desktops, laptops, tablets, smartphones, and other mobile computing devices used by employees—are more vulnerable to Internet-based threats. Use of security controls such as host-based controls (for example, personal firewall software or end-point protection solutions), network-based security controls (for example, firewalls, network-based heuristics inspection, and malware simulation), or hardware, helps to protect devices from Internet-based attacks, which could use the device to gain access to the organization's systems and data when the device reconnects to the network.	X				

PCI DSS Requirements	Guidance
2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. **Customized Approach Objective**	Requirement 2.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 2. While it is important to define the specific policies or procedures called out in Requirement 2, it is equally important to ensure they are properly documented, maintained, and disseminated.
2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood. **Customized Approach Objective**	If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.
2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment. **Customized Approach Objective**	There are known weaknesses with many operating systems, databases, network devices, software, applications, container images, and other devices used by an entity or within an entity's environment. There are also known ways to configure these system components to fix security vulnerabilities. Fixing security vulnerabilities reduces the opportunities available to an attacker. By developing standards, entities ensure their system components will be configured consistently and securely, and address the protection of devices for which full hardening may be more difficult.
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled. **Customized Approach Objective**	Malicious individuals often use vendor default account names and passwords to compromise operating systems, applications, and the systems on which they are installed. Because these default settings are often published and are well known, changing these settings will make systems less vulnerable to attack.

2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	Systems containing a combination of services, protocols, and daemons for their primary function will have a security profile appropriate to allow that function to operate effectively. For example, systems that need to be directly connected to the Internet would have a particular profile, like a DNS server, web server, or an e-commerce server. Conversely, other system components may operate a primary function comprising a different set of services, protocols, and daemons that performs functions that an entity does not want exposed to the Internet. This requirement aims to ensure that different functions do not impact the security profiles of other services in a way which may cause them to operate at a higher or lower security level.
Customized Approach Objective	
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Unnecessary services and functions can provide additional opportunities for malicious individuals to gain access to a system. By removing or disabling all unnecessary services, protocols, daemons, and functions, organizations can focus on securing the functions that are required and reduce the risk that unknown or unnecessary functions will be exploited.
Customized Approach Objective System components cannot be compromised by exploiting unnecessary functionality present in the system component.	
2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to exploit common points of compromise within a network.

Customized Approach Objective System components cannot be compromised by exploiting insecure services, protocols, or daemons.	
2.2.6 System security parameters are configured to prevent misuse. **Customized Approach Objective**	Correctly configuring security parameters provided in system components takes advantage of the capabilities of the system component to defeat malicious attacks.
2.2.7 All non-console administrative access is encrypted using strong cryptography. **Customized Approach Objective**	If non-console (including remote) administration does not use encrypted communications, administrative authorization factors (such as IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data.
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults. **Customized Approach Objective**	If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network. Good Practice Wireless passwords should be constructed so that they are resistant to offline brute force attacks.
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised. **Customized Approach Objective**	Changing wireless encryption keys whenever someone with knowledge of the key leaves the organization or moves to a role that no longer requires knowledge of the key, helps keep knowledge of keys limited to only those with a business need to know. Also, changing wireless encryption keys whenever a key is suspected or known to be comprised makes a wireless network more resistant to compromise.

ystem Components

Control Ownership			Implementation Details	
1800	Client	Shared	1800 Notify	Client
		X	1800 Notify matains security policies that are compliant with PCI DSS	The client must also matain security policies that are compliant with PCI DSS
X				
X				
X				

X				
X				
X				

X				
X				
X				
X				

Protect Stored Account Data						
PCI DSS Requirements	Guidance	Control Ownership			Implementation Details	
		1800	Client	Shared	1800 Notify	Client
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. **Customized Approach Objective** Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Requirement 3.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 3. While it is important to define the specific policies or procedures called out in Requirement 3, it is equally important to ensure they are properly documented, maintained, and disseminated.	X			1800 Notify keeps cardholder data storage to a minimum per PCI DSS requirements.	
3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood. **Customized Approach Objective** Day-to-day responsibilities for performing all the activities in Requirement 3 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.	X				
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. **Customized Approach Objective** Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.	Purpose A formal data retention policy identifies what data needs to be retained, for how long, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only account data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. The storage of SAD data prior to the completion of the authorization process is also included in the data retention and disposal policy so that storage of this sensitive data is kept to minimum, and only retained for the defined amount of time.	X			1800 Notify does not store PAN or SAD data anywhere.	
3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. **Customized Approach Objective** This requirement is not eligible for the customized approach.	SAD is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Therefore, the storage of SAD upon completion of the authorization process is prohibited. The authorization process completes when a merchant receives a transaction response (for example, an approval or decline).	X			1800 Notify does not store PAN or SAD data anywhere.	
3.3.1.1 The full contents of any track are not retained upon completion of the authorization process. **Customized Approach Objective**	If full contents of any track (from the magnetic stripe on the back of a card if present, equivalent data contained on a chip, or elsewhere) is stored, malicious individuals who obtain that data can use it to reproduce payment cards and complete fraudulent transactions.	X			1800 Notify does not store PAN or SAD data anywhere.	
3.3.1.2 The card verification code is not retained upon completion of the authorization process. **Customized Approach Objective**	If card verification code data is stolen, malicious individuals can execute fraudulent Internet and mail-order/telephone-order (MO/TO) transactions. Not storing this data reduces the probability of it being compromised.	X				

3.3.1.3 The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process. **Customized Approach Objective**	PIN and PIN blocks should be known only to the card owner or entity that issued the card. If this data is stolen, malicious individuals can execute fraudulent PIN-based transactions (for example, in-store purchases and ATM withdrawals). Not storing this data reduces the probability of it being	X				
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography. **Customized Approach Objective** This requirement is not eligible for the customized approach.	SAD can be used by malicious individuals to increase the probability of successfully generating counterfeit payment cards and creating fraudulent transactions.	X				
3.3.3 Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. **Applicability Notes** **Customized Approach Objective** Sensitive authentication data is retained only as required to support issuing functions and is secured from unauthorized access.	SAD can be used by malicious individuals to increase the probability of successfully generating counterfeit payment cards and creating fraudulent transactions. Entities should consider encrypting SAD with a different cryptographic key than is used to encrypt PAN. Note that this does not mean that PAN present in SAD (as part of track data) would need to be separately encrypted.	X				
3.4.1 PAN is masked when displayed (the BIN 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 BIN and last four digits of the PAN. **Customized Approach Objective**	The display of full PAN on computer screens, payment card receipts, paper reports, etc. can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that the full PAN is displayed only for those with a legitimate business need minimizes the risk of unauthorized persons gaining access to PAN data.	X				
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. **Customized Approach Objective** PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.	Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN.	X				
3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key-management processes and procedures. **Applicability Notes** **Customized Approach Objective** Cleartext PAN cannot be read from storage media.	The removal of cleartext stored PAN is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control. Secondary independent control systems (for example governing access to, and use of, cryptography and decryption keys) prevent the failure of a primary access control system leading to a breach of confidentiality of stored PAN. If hashing is used to remove stored cleartext PAN, by correlating hashed and truncated versions of a given PAN, a malicious individual can easily derive the original PAN value. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable.	X				
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.	The removal of cleartext stored PAN is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control. Secondary independent control systems (for example governing access to, and use of, cryptography and decryption keys) prevent the failure of a primary access control system leading to a breach of confidentiality of stored PAN.	X				

3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media OR • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1. **Customized Approach Objective**	Disk-level and partition-level encryption typically encrypts the entire disk or partition using the same key, with all data automatically decrypted when the system runs or when an authorized user requests it. For this reason, disk-level encryption is not appropriate to protect stored PAN on computers, laptops, servers, storage arrays, or any other system that provides transparent decryption upon user authentication. Further Information Where available, following vendors' hardening and industry best practice guidelines can assist in securing PAN on these devices.	X				
3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely. **Customized Approach Objective**	Disk-level encryption typically encrypts the entire disk or partition using the same key, with all data automatically decrypted when the system runs or when an authorized user requests it. Many disk-encryption solutions intercept operating system read/write operations and perform the appropriate cryptographic transformations without any special action by the user other than supplying a password or passphrase at system start-up or at the beginning of a session. This provides no protection from a malicious individual that has already managed to gain access to a valid user account.	X				
3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms. ***Applicability Notes*** *This requirement applies to keys used to encrypt stored account data and* **Customized Approach Objective**	Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data. Good Practice Having a centralized key management system based on industry standards is recommended for managing cryptographic keys. Further Information The entity's key management procedures will benefit through alignment with industry requirements, Sources for information on cryptographic key management life cycles include: • ISO 11568-1 Banking — Key management (retail) — Part 1: Principles (specifically Chapter 10 and the referenced Parts 2 & 4) • NIST SP 800-57 Part 1 Revision 5—Recommendation for Key Management - Part 1: General	X				
3.6.1.1 Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4. • Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* ***Applicability Notes*** **Customized Approach Objective**	Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect stored account data, as well as the devices that generate, use, and protect the keys. This allows an entity to keep pace with evolving threats to its architecture and plan for updates as the assurance level provided by different algorithms and key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices and identify unauthorized additions to its cryptographic architecture. The use of the same cryptographic keys in both production and test environments introduces a risk of exposing the key if the test environment is not at the same security level as the production environment.	X				
3.6.1.2 Secret and private keys used to encrypt/decrypt stored account data are stored 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 (SCD), such as a hardware 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. ***Applicability Notes*** *It is not required that public keys be stored in one of these forms.* **Customized Approach Objective**	Storing cryptographic keys securely prevents unauthorized or unnecessary access that could result in the exposure of stored account data. Storing keys separately means they are stored such that if the location of one key is compromised, the second key is not also compromised. Where data-encrypting keys are stored in an HSM, the HSM interaction channel should be protected to prevent interception of encryption or decryption operations.	X				
3.6.1.3 Access to cleartext cryptographic key components is restricted to **Customized Approach Objective**	Restricting the number of people who have access to cleartext cryptographic key components reduces the risk of stored account data	X				
3.7.1 Key-management policies and procedures are implemented to **Customized Approach Objective**	Use of strong cryptographic keys significantly increases the level of security of encrypted account data.	X				
3.7.2 Key-management policies and procedures are implemented to **Customized Approach Objective**	Secure distribution or conveyance of secret or private cryptographic keys means that keys are distributed only to authorized custodians, as	X				

3.7.3 Key-management policies and procedures are implemented to include that cryptographic keys are stored securely. **Customized Approach Objective**	Storing keys without proper protection could provide access to attackers, resulting in the decryption and exposure of account data.	X				
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines. **Customized Approach Objective**	Changing encryption keys when they reach the end of their cryptoperiod is imperative to minimize the risk of someone obtaining the encryption keys	X				
3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations. **Customized Approach Objective** Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.	Keys that are no longer required, keys with weakened integrity, and keys that are known or suspected to be compromised, should be archived, revoked, and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept (for example, to support archived encrypted data), they should be strongly protected.	X				
3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control. **Customized Approach Objective**	Split knowledge and dual control of keys are used to eliminate the possibility of a single person having access to the whole key and therefore being able to gain unauthorized access to the data.	X				
3.7.7 Key management policies and procedures are implemented to include that cryptographic keys are not substituted by unauthorized personnel. **Customized Approach Objective** Cryptographic keys cannot be substituted by unauthorized personnel.	If an attacker is able to substitute an entity's key with a key the attacker knows, the attacker will be able to decrypt all data encrypted with that key.	X				
3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities. **Customized Approach Objective** Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.	This process will help ensure individuals that act as key custodians commit to the key-custodian role and understand and accept the responsibilities. An annual reaffirmation can help remind key custodians of their responsibilities.	X				
3.7.9 Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers. **Customized Approach Objective**	Providing guidance to customers on how to securely transmit, store, and update cryptographic keys can help prevent keys from being mismanaged or disclosed to unauthorized entities.	X				

P
PCI DSS Requirements
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.
Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 4 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.
Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 4 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks:
• Only trusted keys and certificates are accepted.
• The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.
• The encryption strength is appropriate for the encryption methodology in use.
• Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until its effective date; refer to applicability notes below for details.*

Applicability Notes
There could be occurrences where an entity receives cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of receiving sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or implement measures to prevent the channel from being used for cardholder data.

A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organization, the certificate's author is confirmed, and the certificate is verified—for example, via hash or signature—and has not expired. Note that self-signed certificates where the Distinguished Name (DN) field in the "issued by" and "issued to" field is the same are not acceptable.

Customized Approach Objective
Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.

4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.

Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Customized Approach Objective
All keys and certificates used to protect PAN during transmission are identified and confirmed as trusted.

4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.

Customized Approach Objective
Cleartext PAN cannot be read or intercepted from wireless network transmissions.

4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.

Applicability Notes

This requirement also applies if a customer, or other third-party, requests that PAN is sent to them via end-user messaging technologies.

There could be occurrences where an entity receives unsolicited cardholder data via an insecure communication channel that was not intended for transmissions of sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or delete the cardholder data and implement measures to prevent the channel from being used for cardholder data.

Customized Approach Objective

Cleartext PAN cannot be read or intercepted from transmissions using end-user messaging technologies.

rotect Cardholder Data with Strong Cryptography During Transmission Over Open,

Guidance	Control Ownership		
	1800 Notify	Client	Shared
Requirement 4.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 4. While it is important to define the specific policies or procedures called out in Requirement 4, it is equally important to ensure they are properly documented, maintained, and disseminated.			X
If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.	X		

Sensitive information must be encrypted during transmission over public networks because it is easy and common for a malicious individual to intercept and/or divert data while in transit. PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both. While it is not required that strong cryptography be applied at both the data level and the session level, it is strongly recommended. If encrypted at the data level, the cryptographic keys used for protecting the data can be managed in accordance with Requirements 3.6 and 3.7. If the data is encrypted at the session level, designated key custodians should be assigned responsibility for managing transmission keys and certificates.	X		
The inventory of trusted keys helps the entity keep track of the algorithms, protocols, key strength, key custodians, and key expiry dates. This enables the entity to respond quickly to vulnerabilities discovered in encryption software, certificates, and cryptographic algorithms.	X		
Since wireless networks do not require physical media to connect, it is important to establish controls limiting who can connect and what transmission protocols will be used. Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks.	X		

End-user messaging technologies typically can be easily intercepted by packet-sniffing during delivery across internal and public networks. The use of end-user messaging technology to send PAN should only be considered where there is a defined business need.	X		

Public Networks	
Implementation Details	
1800 Notify	**Client**
1800 Notify maintains strong PCI DSS cryptograpy requirement protocols.	The Client must also maintain strong PCI DSS cryptograpy requirement protocols.

PCI DSS Requirements	Guidance
5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. **Customized Approach Objective** Expectations, controls, and oversight for meeting activities within Requirement 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Requirement 5.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 5. While it is important to define the specific policies or procedures called out in Requirement 5, it is equally important to ensure they are properly documented, maintained, and disseminated.
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood. **Customized Approach Objective** Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	If roles and responsibilities are not formally assigned, networks and systems may not be properly protected from malware.
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware. **Customized Approach Objective** Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.	There is a constant stream of attacks targeting newly discovered vulnerabilities in systems previously regarded as secure. Without an anti-malware solution that is updated regularly, new forms of malware can be used to attack systems, disable a network, or compromise data.
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware. **Customized Approach Objective** Malware cannot execute or infect other system components.	Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning.

5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection. ***Applicability Notes*** *System components covered by this requirement are those for which there is no anti-malware solution deployed per Req 5.2.1.* **Customized Approach Objective** The entity maintains awareness of evolving malware threats to ensure that any systems not protected from malware are not at risk of infection.	Certain systems, at a given point in time, may not currently be commonly targeted or affected by malware. However, industry trends for malware can change quickly, so it is important for organizations to be aware of new malware that might affect their systems—for example, by monitoring vendor security notices and anti-malware forums to determine whether its systems might be coming under threat from new and evolving malware.
5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ***Applicability Notes*** *This requirement applies to entities conducting periodic malware scans to meet Req 5.3.2.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Systems not known to be at risk from malware are re-evaluated at a frequency that addresses the entity's risk.	Entities determine the optimum period to undertake the evaluation based on criteria such as the complexity of each entity's environment and the number of types of systems that are required to be evaluated.
5.3.1 The anti-malware solution(s) is kept current via automatic updates. **Customized Approach Objective** Anti-malware mechanisms can detect and address the latest malware threats.	For an anti-malware solution to remain effective, it needs to have the latest security updates, signatures, threat analysis engines, and any other malware protections on which the solution relies. Having an automated update process avoids burdening end users with responsibility for manually installing updates and provides greater

5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. OR • Performs continuous behavioral analysis of systems or processes. **Customized Approach Objective** Malware cannot complete execution.	Periodic scans can identify malware that is present, but currently inactive, within the environment. Some malware, such as zero-day malware, can enter an environment before the scan solution is capable of detecting it. Performing regular periodic scans or continuous behavioral analysis of systems or processes helps ensure that previously undetectable malware can be identified, removed, and investigated to determine how it gained
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ***Applicability Notes*** *This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Scans by the malware solution are performed at a frequency that addresses the entity's risk.	Entities can determine the optimum period to undertake periodic scans based on their own assessment of the risks posed to their environments.
5.3.3 For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Portable media devices are often overlooked as an entry method for malware. Attackers will often pre-load malware onto portable devices such as USB and flash drives; connecting an infected device to a computer then triggers the malware, introducing new threats within the environment.

Customized Approach Objective Malware cannot be introduced to system components via external removable media.	
5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	It is important to track the effectiveness of the anti-malware mechanisms—for example, by confirming that updates and scans are being performed as expected, and that malware is identified and addressed. Audit logs also allow an entity to determine how malware entered the environment and track its activity when inside the entity's network.
Customized Approach Objective Historical records of anti-malware actions are immediately available and retained for at least 12 months.	
5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period. ***Applicability Notes*** *Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which anti-malware protection is not active.*	It is important that defensive mechanisms are always running so that malware is detected in real time. Ad-hoc starting and stopping of anti-malware solutions could allow malware to propagate unchecked and undetected.
Customized Approach Objective Anti-malware mechanisms cannot be modified by unauthorized personnel.	

5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. ***Applicability Notes*** *This requirement applies to the automated mechanism. It is not intended that the systems and services providing such automated mechanisms (such as email servers) are brought into scope for PCI DSS.* *The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS.* *Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Req 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Mechanisms are in place to protect against and mitigate risk posed by phishing attacks.	Technical controls can limit the number of occasions personnel have to evaluate the veracity of a communication and can also limit the effects of individual responses to phishing.

n Malicious Software

Control Ownership			Implementation Details	
1800 Notify	Client	Shared	1800 Notify	Client
		X	1800 Notify matains security policies and operational procedures that are compliant with PCI DSS	The client must also matain security policies and operational procedures that are compliant with PCI DSS
X				
X				
X				

X				
X				
X				

X				
X				
X				

X				
X				

X				

PCI DSS Requirements
6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.
Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 6 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.
Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 6 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle. ***Applicability Notes*** *This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.*
Customized Approach Objective Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.
6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

Customized Approach Objective
Software development personnel remain knowledgeable about secure development practices; software security; and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.

6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows:
• Code reviews ensure code is developed according to secure coding guidelines.
• Code reviews look for both existing and emerging software vulnerabilities.
• Appropriate corrections are implemented prior to release.

Applicability Notes
This requirement for code reviews applies to all bespoke and custom software (both internal and public-facing), as part of the system development lifecycle.
Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.4.
Code reviews may be performed using either manual or automated processes, or a combination of both.

Customized Approach Objective
Bespoke and custom software cannot be exploited via coding vulnerabilities.

6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:
• Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.
• Reviewed and approved by management prior to release.

Applicability Notes
Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel.
An individual that has been formally granted accountability for release control and who is neither the original code author nor the code reviewer fulfills the criteria of being management.

Customized Approach Objective
The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.

6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:

- Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.
- Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.
- Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.
- Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).
- Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.
- Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

Applicability Notes

This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.

Customized Approach Objective

Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.

6.3.1 Security vulnerabilities are identified and managed as follows:
• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Applicability Notes
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Req 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.

Customized Approach Objective
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.

6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.

Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Customized Approach Objective
Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.

6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:
• Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
• All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).

Customized Approach Objective
System components cannot be compromised via the exploitation of a known vulnerability.

6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:

• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:

– At least once every 12 months and after significant changes.

– By an entity that specializes in application security.

– Including, at a minimum, all common software attacks in Requirement 6.2.4.

– All vulnerabilities are ranked in accordance with requirement 6.3.1.

– All vulnerabilities are corrected.

– The application is re-evaluated after the corrections

OR

• Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:

– Installed in front of public-facing web applications to detect and prevent web-based attacks.

– Actively running and up to date as applicable.

– Generating audit logs.

– Configured to either block web-based attacks or generate an alert that is immediately investigated.

Applicability Notes

This assessment is not the same as the vulnerability scans performed for Req 11.3.1 and 11.3.2.

This requirement will be superseded by Requirement 6.4.2 after 31 March

Customized Approach Objective

Public-facing web applications are protected against malicious attacks.

6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:

• Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.

• Actively running and up to date as applicable.

• Generating audit logs.

• Configured to either block web-based attacks or generate an alert that is immediately investigated.

Applicability Notes

This new requirement will replace Req 6.4.1 once its effective date is reached.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Customized Approach Objective Public-facing web applications are protected in real time against malicious attacks.
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary. ***Applicability Notes*** *This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*
Customized Approach Objective Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.
6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.
Customized Approach Objective All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable. ***Applicability Notes*** *These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmation activity per Req 12.5.2.*
Customized Approach Objective All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.

6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.
Customized Approach Objective Pre-production environments cannot introduce risks and vulnerabilities into production environments.
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed. ***Applicability Notes*** *In environments with limited personnel where individuals perform multiple roles or functions, this same goal can be achieved with additional procedural controls that provide accountability. For example, a developer may also be an administrator that uses an administrator-level account with elevated privileges in the development environment and, for their developer role, they use a separate account with user-level access to the production environment.*
Customized Approach Objective Job roles and accountability that differentiate between pre-production and production activities are defined and managed to minimize the risk of unauthorized, unintentional, or inappropriate actions.
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.
Customized Approach Objective Live PANs cannot be present in pre-production environments outside the CDE.
6.5.6 Test data and test accounts are removed from system components before the system goes into production.
Customized Approach Objective Test data and test accounts cannot exist in production environments.

Develop and Maintain Secure Systems and Software

Guidance	Control Ownership		
	1800 Notify	Client	Shared
Requirement 6.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 6. While it is important to define the specific policies or procedures called out in Requirement 6, it is equally important to ensure they are properly documented, maintained, and disseminated.			X
If roles and responsibilities are not formally assigned, systems will not be securely maintained, and their security level will be reduced.	X		
Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment.	X		
Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.	X		

Security vulnerabilities in bespoke and custom software are commonly exploited by malicious individuals to gain access to a network and compromise account data. Vulnerable code is far more difficult and expensive to address after it has been deployed or released into production environments. Requiring a formal review and signoff by management prior to release helps to ensure that code is approved and has been developed in accordance with policies and procedures.	X		
Having code reviewed by someone other than the original author, who is both experienced in code reviews and knowledgeable about secure coding practices, minimizes the possibility that code containing security or logic errors that could affect the security of cardholder data is released into a production environment. Requiring management approval that the code was reviewed limits the ability for the process to be bypassed.	X		

Detecting or preventing common errors that result in vulnerable code as early as possible in the software development process lowers the probability that such errors make it through to production and lead to a compromise. Having formal engineering techniques and tools embedded in the development process will catch these errors early. This philosophy is sometimes called “shifting security left.”	X		

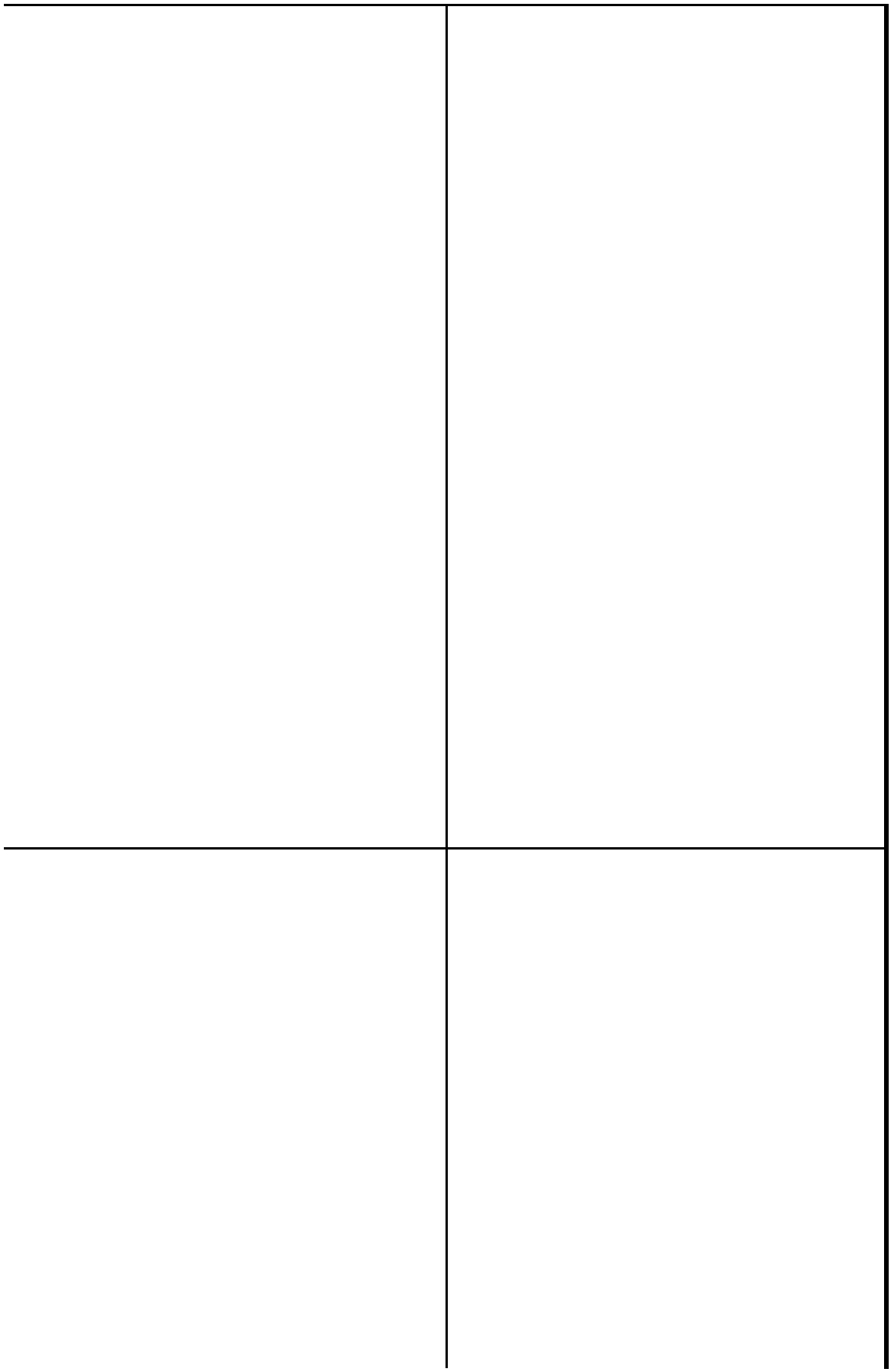
Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.	X		
Identifying and listing all the entity's bespoke and custom software, and any third-party software that is incorporated into the entity's bespoke and custom software enables the entity to manage vulnerabilities and patches.	X		
New exploits are constantly being discovered, and these can permit attacks against systems that have previously been considered secure. If the most recent security patches/updates are not implemented on critical systems as soon as possible, a malicious actor can use these exploits to attack or disable a system or gain access to sensitive data.	X		

Public-facing web applications are those that are available to the public (not only for internal use). These applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities. Common assessment tools include specialized web scanners that perform automatic analysis of web application protection. When using automated technical solutions, it is important to include processes that facilitate timely responses to alerts generated by the solutions so that any detected attacks can be mitigated.	X		
Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems.	X		

Scripts loaded and executed in the payment page can have their functionality altered without the entity's knowledge and can also have the functionality to load additional external scripts (for example, advertising and tracking, tag management systems). Such seemingly harmless scripts can be used by potential attackers to upload malicious scripts that can read and exfiltrate cardholder data from the consumer browser.	X		
Change management procedures must be applied to all changes—including the addition, removal, or modification of any system component—in the production environment. It is important to document the reason for a change and the change description so that relevant parties understand and agree the change is needed. Likewise, documenting the impacts of the change allows all affected parties to plan appropriately for any processing changes.	X		
Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment, and that PCI DSS requirements continue to be met to secure the environment.	X		

Due to the constantly changing state of pre-production environments, they are often less secure than the production environment.	X		
The goal of separating roles and functions between production and pre-production environments is to reduce the number of personnel with access to the production environment and account data and thereby minimize risk of unauthorized, unintentional, or inappropriate access to data and system components and help ensure that access is limited to those individuals with a business need for such access.	X		
Use of live PANs outside of protected CDEs provides malicious individuals with the opportunity to gain unauthorized access to cardholder data. Entities can minimize their storage of live PANs by only storing them in pre-production when strictly necessary for a specific and defined testing purpose and securely deleting that data after use.	X		
This data may give away information about the functioning of an application or system and is an easy target for unauthorized individuals to exploit to gain access to systems. Possession of such information could facilitate compromise of the system and related account data.	X		

Implementation Details	
1800 Notify	**Client**
1800 Notify matains security policies and operational procedures that are compliant with PCI DSS	The client must also matain security policies and operational procedures that are compliant with PCI DSS



PCI DSS Requirements	Guidance
7.1.1 All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. **Customized Approach Objective** Expectations, controls, and oversight for meeting activities within Requirement 7 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Requirement 7.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 7. While it is important to define the specific policies or procedures called out in Requirement 7, it is equally important to ensure they are properly documented, maintained, and disseminated.
7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood. **Customized Approach Objective** Day-to-day responsibilities for performing all the activities in Requirement 7 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur.
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function. **Customized Approach Objective** Access requirements are established according to job functions following least-privilege and need-to-know principles.	Defining an access control model that is appropriate for the entity's technology and access control philosophy supports a consistent and uniform way of allocating access and reduces the possibility of errors such as the granting of excessive rights.

7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities. **Customized Approach Objective** Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.	Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID.
7.2.3 Required privileges are approved by authorized personnel. **Customized Approach Objective** Access privileges cannot be granted to users without appropriate, documented authorization.	Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.
7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate. **Customized Approach Objective** Account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.	Regular review of access rights helps to detect excessive access rights remaining after user job responsibilities change, system functions change, or other modifications. If excessive user rights are not revoked in due time, they may be used by malicious users for unauthorized access. This review provides another opportunity to ensure that accounts for all terminated users have been removed (if any were missed at the time of termination), as well as to ensure that any third parties that no longer need access have had their access terminated.
7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Access rights granted to application and system accounts are limited to only the access needed for the operability of that application or system.	It is important to establish the appropriate access level for application or system accounts. If such accounts are compromised, malicious users will receive the same access level as that granted to the application or system. Therefore, it is important to ensure limited access is granted to system and application accounts on the same basis as to user accounts.

7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Application and system account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.	Regular review of access rights helps to detect excessive access rights remaining after system functions change, or other application or system modifications occur. If excessive rights are not removed when no longer needed, they may be used by malicious users for unauthorized access.
7.2.6 All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD. ***Applicability Notes*** *This requirement applies to controls for user access to query repositories of stored cardholder data.* *See Req 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.* **Customized Approach Objective** Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator.	The misuse of query access to repositories of cardholder data has been a regular cause of data breaches. Limiting such access to administrators reduces the risk of such access being abused by unauthorized users.

7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components. **Customized Approach Objective** Access rights and privileges are managed via mechanisms intended for that purpose.	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges.
7.3.2 The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function. **Customized Approach Objective** Individual account access rights and privileges to systems, applications, and data are only inherited from group membership.	Restricting privileged access with an access control system reduces the opportunity for errors in the assignment of permissions to individuals, applications, and systems.
7.3.3 The access control system(s) is set to "deny all" by default. **Customized Approach Objective** Access rights and privileges are prohibited unless expressly permitted.	A default setting of "deny all" ensures no one is granted access unless a rule is established specifically granting such access. It is important to check the default configuration of access control systems

ler Data by Business Need to Know

Control Ownership			Implementation Details	
1800 Notify	Client	Shared	1800 Notify	Client
		X	1800 Notify matains security policies that are compliant with PCI DSS	The client must also matain security policies that are compliant with PCI DSS
X				
X				

X				
X				
X				
X				

X				
X				

X				
X				
X				

PCI DSS Requirements
8.1.1 All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.
Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.
Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 8 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed. ***Applicability Notes*** *This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).*
Customized Approach Objective All actions by all users are attributable to an individual.

8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:
• Account use is prevented unless needed for an exceptional circumstance.
• Use is limited to the time needed for the exceptional circumstance.
• Business justification for use is documented.
• Use is explicitly approved by management.
• Individual user identity is confirmed before access to an account is granted.
• Every action taken is attributable to an individual user.

Applicability Notes
This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

Customized Approach Objective
All actions performed by users with generic, system, or shared IDs are attributable to an individual person.

8.2.3 Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.

Applicability Notes
This requirement is not intended to apply to service providers accessing their own shared services environments, where multiple customer environments are hosted.

If service provider employees use shared authentication factors to remotely access customer premises, these factors must be unique per customer and managed in accordance with Req 8.2.2.

This requirement applies only when the entity being assessed is a service provider.

Customized Approach Objective
A service provider's credential used for one customer cannot be used for any other customer.

8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:
• Authorized with the appropriate approval.
• Implemented with only the privileges specified on the documented approval.

Applicability Notes
This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers and third-party vendors.

Customized Approach Objective
Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.

8.2.5 Access for terminated users is immediately revoked.

Customized Approach Objective
The accounts of terminated users cannot be used.

8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:
• Enabled only during the time period needed and disabled when not in use.
• Use is monitored for unexpected activity.

Customized Approach Objective
Third party remote access cannot be used except where specifically authorized and use is overseen by management.

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

Applicability Notes
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).
This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.

Customized Approach Objective
A user session cannot be used except by the authorized user.

8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:
• 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 element.

Applicability Notes
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).
This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements.

A digital certificate is a valid option for "something you have" if it is unique for a particular user.

Customized Approach Objective
An account cannot be accessed except with a combination of user identity and an authentication factor.

8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.

Customized Approach Objective
Cleartext authentication factors cannot be obtained, derived, or reused from the interception of communications or from stored data.

8.3.3 User identity is verified before modifying any authentication factor.

Customized Approach Objective
Unauthorized individuals cannot gain system access by impersonating the identity of an authorized user.

8.3.4 Invalid authentication attempts are limited by:
• Locking out the user ID after not more than 10 attempts.
• Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.

Applicability Notes
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

Customized Approach Objective
An authentication factor cannot be guessed in a brute force, online attack.

8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:
• Set to a unique value for first-time use and upon reset.
• Forced to be changed immediately after the first use.

Customized Approach Objective
An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.

8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:
• A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
• Contain both numeric and alphabetic characters.

Applicability Notes
This requirement is not intended to apply to:
• User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals)
• Application or system accounts, which are governed by requirements in section 8.6

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3

Customized Approach Objective
A guessed password/passphrase cannot be verified by either an online or offline brute force attack.

8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.

Applicability Notes
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

Customized Approach Objective
A previously used password cannot be used to gain access to an account for at least 12 months.

8.3.8 Authentication policies and procedures are documented and communicated to all users including:
• Guidance on selecting strong authentication factors.
• Guidance for how users should protect their authentication factors.
• Instructions not to reuse previously used passwords/passphrases.
• Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.

Customized Approach Objective
Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.

8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:
• Passwords/passphrases are changed at least once every 90 days,
OR
• The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

Applicability Notes
This requirement applies to in-scope system components that are not in the CDE because these components are not subject to MFA requirements. This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.

Customized Approach Objective
An undetected compromised password/passphrase cannot be used indefinitely.

8.3.10 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including:

• Guidance for customers to change their user passwords/passphrases periodically.

• Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.

Applicability Notes

This requirement does not apply to accounts of consumer users accessing their own payment card information.

This requirement applies only when the entity being assessed is a service provider.

This requirement for service providers will be superseded by Requirement 8.3.10.1, as of 31 March 2025

Customized Approach Objective

Passwords/passphrases for service providers' customers cannot be used indefinitely.

8.3.10.1 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either:

• Passwords/passphrases are changed at least once every 90 days,

OR

• The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

Applicability Notes

This requirement does not apply to accounts of consumer users accessing their own payment card information.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Until this requirement is effective on 31 March 2025, service providers may meet either Requirement 8.3.10 or 8.3.10.1.

Customized Approach Objective

Passwords/passphrases for service providers' customers cannot be used indefinitely.

8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.
Customized Approach Objective An authentication factor cannot be used by anyone other than the user to which it is assigned.
8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access. ***Applicability Notes*** *The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection—that is, via logical access occurring over a network interface rather than via a direct, physical connection.* *MFA is considered a best practice for non-console administrative access to in-scope system components that are not part of the CDE .*
Customized Approach Objective Administrative access to the CDE cannot be obtained by the use of a single authentication factor.

8.4.2 MFA is implemented for all access into the CDE.

Applicability Notes

This requirement does not apply to:

- *Application or system accounts performing automated functions*
- *User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals)*

MFA is required for both types of access specified in Req 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting via non-console administrative access from the entity's network into the CDE.

The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.

MFA for remote access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels.

Customized Approach Objective

Access into the CDE cannot be obtained by the use of a single authentication factor.

8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows:
• All remote access by all personnel, both users and administrators, originating from outside the entity's network.
• All remote access by third parties and vendors.

Applicability Notes
The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE.
If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity's networks.
The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.

Customized Approach Objective
Remote access to the entity's network cannot be obtained by using a single authentication factor.

8.5.1 MFA systems are implemented as follows:
• The MFA system is not susceptible to replay attacks.
• MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period.
• At least two different types of authentication factors are used.
• Success of all authentication factors is required before access is granted.

Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Customized Approach Objective
MFA systems are resistant to attack and strictly control any administrative overrides.

8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows:
• Interactive use is prevented unless needed for an exceptional circumstance.
• Interactive use is limited to the time needed for the exceptional circumstance.
• Business justification for interactive use is documented.
• Interactive use is explicitly approved by management.
• Individual user identity is confirmed before access to account is granted.
• Every action taken is attributable to an individual user.

Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Customized Approach Objective
When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.

8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.

Applicability Notes
Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Req 8.3.2.
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Customized Approach Objective
Passwords/passphrases used by application and system accounts cannot be used by unauthorized personnel.

8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:

• Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise.

• Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Customized Approach Objective

Passwords/passphrases used by application and system accounts cannot be used indefinitely and are structured to resist brute-force and guessing attacks.

Identify Users and Authenticate Access to System Components

Guidance	Control Ownership		
	1800 Notify	Client	Shared
Requirement 8.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 8. While it is important to define the specific policies or procedures called out in Requirement 8, it is equally important to ensure they are properly documented, maintained, and disseminated.			X
If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.	X		
The ability to trace actions performed on a computer system to an individual establishes accountability and traceability and is fundamental to establishing effective access controls. By ensuring each user is uniquely identified, instead of using one ID for several employees, an organization can maintain individual responsibility for actions and an effective record in the audit log per employee. In addition, this will assist with issue resolution and containment when misuse or malicious intent occurs.	X		

Group, shared, or generic (or default) accounts are typically delivered with software or operating systems—for example, root or with privileges associated with a specific function, such as an administrator. If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. In turn, this prevents an entity from assigning accountability for, or having effective logging of, an individual's actions since a given action could have been performed by anyone in the group with knowledge of the user ID and associated authentication factors.	X		
Service providers with remote access to customer premises typically use this access to support POS POI systems or provide other remote services. If a service provider uses the same authentication factors to access multiple customers, all the service provider's customers can easily be compromised if an attacker compromises that one factor.	X		

It is imperative that the lifecycle of a user ID (additions, deletions, and modifications) is controlled so that only authorized accounts can perform functions, actions are auditable, and privileges are limited to only what is required. Attackers often compromise an existing account and then escalate the privileges of that account to perform unauthorized acts, or they may create new IDs to continue their activity in the background. It is essential to detect and respond when user accounts are created or changed outside the normal change process or without corresponding authorization.	X		
If an employee or third party/vendor has left the company and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur—either by the former employee or	X		
Allowing third parties to have 24/7 access into an entity's systems and networks in case they need to provide support increases the chances of unauthorized access. This access could result in an unauthorized user in the third party's environment or a malicious individual using the always-available external entry point into an entity's network. Where third parties do need access 24/7, it should be documented, justified, monitored, and tied to specific service reasons.	X		
When users walk away from an open machine with access to system components or cardholder data, there is a risk that the machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse.	X		

When used in addition to unique IDs, an authentication factor helps protect user IDs from being compromised, since the attacker needs to have the unique ID and compromise the associated authentication factor(s).	X		
Network devices and applications have been known to transmit unencrypted, readable authentication factors (such as passwords and passphrases) across the network and/or store these values without encryption. As a result, a malicious individual can easily intercept this information during transmission using a “sniffer,” or directly access	X		
Malicious individuals use "social engineering” techniques to impersonate a user of a system —for example, calling a help desk and acting as a legitimate user—to have an authentication factor changed so they can use a valid user ID. Requiring positive identification of a user reduces the probability of this	X		
Without account-lockout mechanisms in place, an attacker can continually try to guess a password through manual or automated tools (for example, password cracking) until the attacker succeeds and gains access to a user’s account.	X		

If the same password/passphrase is used for every new user, an internal user, former employee, or malicious individual may know or easily discover the value and use it to gain access to accounts before the authorized user attempts to use the password.	X		
Strong passwords/passphrases may be the first line of defense into a network since a malicious individual will often first try to find accounts with weak, static, or non-existent passwords. If passwords are short or easily guessable, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID.	X		
If password history is not maintained, the effectiveness of changing passwords is reduced, as previous passwords can be reused over and over. Requiring that passwords cannot be reused for a period reduces the likelihood that passwords that have been guessed or brute-forced will be re-used in the future.	X		

Communicating authentication policies and procedures to all users helps them to understand and abide by the policies. Good Practice Guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that do not contain dictionary words or information about the user, such as the user ID, names of family members, date of birth, etc.	X		
Access to in-scope system components that are not in the CDE may be provided using a single authentication factor, such as a password/passphrase, token device or smart card, or biometric attribute. Where passwords/passphrases are employed as the only authentication factor for such access, additional controls are required to protect the integrity of the password/passphrase.	X		

Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase.	X		
Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase.	X		

If multiple users can use authentication factors such as tokens, smart cards, and certificates, it may be impossible to identify the individual using the authentication mechanism.	X		
Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase.	X		

Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase.	X		

Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows, such as a password or passphrase.	X		
Poorly configured MFA systems can be bypassed by attackers. This requirement therefore addresses configuration of MFA system(s) that provide MFA for users accessing system components in the CDE. Using one type of factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	X		

Like individual user accounts, system and application accounts require accountability and strict management to ensure they are used only for the intended purpose and are not misused. Attackers often compromise system or application accounts to gain access to cardholder data.	X		
Not properly protecting passwords/passphrases used by application and system accounts, especially if those accounts can be used for interactive login, increases the risk and success of unauthorized use of those privileged accounts.	X		

Systems and application accounts pose more inherent security risk than user accounts because they often run in an elevated security context, with access to systems that may not be typically granted to user accounts, such as programmatic access to databases, etc. As a result, special consideration must be made to protect passwords/passphrases used for application and system accounts.	X		

Implementation Details	
1800 Notify	**Client**
1800 Notify implements PCI compliant controls for all accounts with access to the cardholder data environment.	Client must also implement PCI compliant controls for all users who have access to the cardholder data envrionment including the 1800 Notify Secure Portal users.

PCI DSS Requirements
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.
Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.
Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.
Customized Approach Objective System components in the CDE cannot be physically accessed by unauthorized personnel.
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.
Customized Approach Objective Trusted, verifiable records are maintained of individual physical entry to, and exit from, sensitive areas.
9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.
Customized Approach Objective Unauthorized devices cannot connect to the entity's network from public areas within the facility.

9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.
Customized Approach Objective Physical networking equipment cannot be accessed by unauthorized personnel.
9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.
Customized Approach Objective Physical consoles within sensitive areas cannot be used by unauthorized personnel.
9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.
Customized Approach Objective Requirements for access to the physical CDE are defined and enforced to identify and authorize personnel.
9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.
Customized Approach Objective Sensitive areas cannot be accessed by unauthorized personnel.
9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.
Customized Approach Objective Requirements for visitor access to the CDE are defined and enforced. Visitors cannot exceed any authorized physical access allowed while in the CDE.
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.
Customized Approach Objective Visitor identification or badges cannot be reused after expiration.

9.3.4 A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.
Customized Approach Objective Records of visitor access that enable the identification of individuals are maintained.
9.4.1 All media with cardholder data is physically secured.
Customized Approach Objective Media with cardholder data cannot be accessed by unauthorized personnel.
9.4.1.1 Offline media backups with cardholder data are stored in a secure location.
Customized Approach Objective Offline backups cannot be accessed by unauthorized personnel.
9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.
Customized Approach Objective The security controls protecting offline backups are verified periodically by inspection.
9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.
Customized Approach Objective Media are classified and protected appropriately.
9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.
Customized Approach Objective Media is secured and tracked when transported outside the facility.
9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). ***Applicability Notes*** *Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have "manager" as part of their title.*

Customized Approach Objective Media cannot leave a facility without the approval of accountable personnel.
9.4.5 Inventory logs of all electronic media with cardholder data are maintained.
Customized Approach Objective Accurate inventories of stored electronic media are maintained.
9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.
Customized Approach Objective Media inventories are verified periodically.
9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction. ***Applicability Notes*** *These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Req 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.*
Customized Approach Objective Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.
9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed. ***Applicability Notes*** *These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Req 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.*
Customized Approach Objective Cardholder data cannot be recovered from media that has been erased or destroyed.

9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:
• Maintaining a list of POI devices.
• Periodically inspecting POI devices to look for tampering or unauthorized substitution.
• Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

Customized Approach Objective
The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.

9.5.1.1 An up-to-date list of POI devices is maintained, including:
• Make and model of the device.
• Location of device.
• Device serial number or other methods of unique identification.

Applicability Notes
These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped). This requirement is not intended to apply to manual PAN key-entry components such as computer keyboards.

This requirement is recommended, but not required, for manual PAN key-entry components such as computer keyboards.
This requirement does not apply to commercial off- the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.

Customized Approach Objective
The identity and location of POI devices is recorded and known at all times.

9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.

Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Customized Approach Objective
Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.

9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*
Customized Approach Objective POI devices are inspected at a frequency that addresses the entity's risk.
9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.
Customized Approach Objective Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.

Restrict Physical Access to Cardholder Data

Guidance	Control Ownership		
	1800 Notify	Client	Shared
Requirement 9.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 9. While it is important to define the specific policies or procedures called out in Requirement 9, it is equally important to ensure they are properly documented, maintained, and disseminated.			X
If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur.	X		
Without physical access controls, unauthorized persons could potentially gain access to the CDE and sensitive information, or could alter system configurations, introduce vulnerabilities into the network, or destroy or steal equipment. Therefore, the purpose of this requirement is that physical access to the CDE is controlled via physical security controls such	X		
exiting the sensitive areas can help with investigations of physical breaches by identifying individuals that physically accessed the sensitive areas, as well as when they entered and exited. Whichever mechanism meets this requirement, it should effectively monitor all entry and exit points to sensitive areas.	X		
Restricting access to network jacks (or network ports) will prevent malicious individuals from plugging into readily available network jacks and gaining access to the CDE or systems connected to the CDE.	X		

Without appropriate physical security over access to wireless components and devices, and computer networking and telecommunications equipment and lines, malicious users could gain access to the entity's network resources. Additionally, they could connect their own devices to the network to gain unauthorized access to the CDE or systems connected to the CDE.	X		
Locking console login screens prevents unauthorized persons from gaining access to sensitive information, altering system configurations, introducing vulnerabilities into the network, or destroying records.	X		
Establishing procedures for granting, managing, and removing access when it is no longer needed ensures non-authorized individuals are prevented from gaining access to areas containing cardholder data. In addition, it is important to limit access to the actual badging system and badging materials to prevent unauthorized personnel from making their own badges and/or setting up their own access rules.	X		
Controlling physical access to sensitive areas helps ensure that only authorized personnel with a legitimate business need are granted access. Where possible, organizations should have policies and procedures to ensure that before personnel leaving the organization, all physical access mechanisms are returned, or disabled as soon as possible upon their departure. This will ensure personnel cannot gain physical access to sensitive areas once their employment has ended.	X		
Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to facilities and potentially to cardholder data. Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.	X		
Ensuring that visitor badges are returned or deactivated upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended.	X		

A visitor log documenting minimum information about the visitor is easy and inexpensive to maintain. It will assist in identifying historical physical access to a building or room and potential access to cardholder data.	X		
Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media,	X		
If stored in a non-secured facility, backups containing cardholder data may easily be lost, stolen, or copied for malicious intent.	X		
Conducting regular reviews of the storage facility enables the organization to address identified security issues promptly, minimizing the potential risk. It is important for the entity to be aware of the security of the area where media is being stored.	X		
Media not identified as confidential may not be adequately protected or may be lost or stolen.	X		
Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. The use of secure couriers to deliver any media that contains cardholder data allows organizations to use their tracking systems to maintain inventory and location of shipments.	X		
Without a firm process for ensuring that all media movements are approved before the media is removed from secure areas, the media would not be tracked or appropriately protected, and its location would be unknown, leading to lost or stolen media.	X		

Without careful inventory methods and storage controls, stolen or missing electronic media could go unnoticed for an indefinite amount of time.	X		
Without careful inventory methods and storage controls, stolen or missing electronic media could go unnoticed for an indefinite amount of time.	X		
If steps are not taken to destroy information contained on hard-copy media before disposal, malicious individuals may retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as “dumpster diving,” where they search through trashcans and recycle bins looking for hard-copy materials with information they can use to launch an attack.	X		
If steps are not taken to destroy information contained on electronic media when no longer needed, malicious individuals may retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as “dumpster diving,” where they search through trashcans and recycle bins looking for information they can use to launch an attack.	X		

Criminals attempt to steal payment card data by stealing and/or manipulating card-reading devices and terminals. Criminals will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card data every time a card is entered. They will also try to add "skimming" components to the outside of devices, which are designed to capture payment card data before it enters the device—for example, by attaching an additional card reader on top of the legitimate card reader so that the payment card data is captured twice: once by the criminal's component and then by the device's legitimate component. In this way, transactions may still be completed without interruption while the criminal is "skimming" the payment card data during the process.	X		
Keeping an up-to-date list of POI devices helps an organization track where devices are supposed to be and quickly identify if a device is missing or lost.	X		
Regular inspections of devices will help organizations detect tampering more quickly via external evidence—for example, the addition of a card skimmer—or replacement of a device, thereby minimizing the potential impact of using fraudulent devices.	X		

Entities are best placed to determine the frequency of POI device inspections based on the environment in which the device operates.	X		
Personnel training should include being alert to and questioning anyone who shows up to do POI maintenance to ensure they are authorized and have a valid work order, including any agents, maintenance or repair personnel, technicians, service providers, or other third parties. All third parties requesting access to devices should always be verified before being provided access—for example, by checking with management or phoning the POI maintenance company, such as the vendor or acquirer, for verification. Many criminals will try to fool personnel by dressing for the part (for example, carrying toolboxes and dressed in work apparel), and could also be knowledgeable about locations of devices, so personnel should be trained to always follow procedures.	X		

Implementation Details	
1800 Notify	**Client**
1800 Notify matains operational procedures that are compliant with PCI DSS	The client must also matain operational procedures that are compliant with PCI DSS

PCI DSS Requirements	Guidance
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. **Customized Approach Objective** Expectations, controls, and oversight for meeting activities within Requirement 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Requirement 10.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 10. While it is important to define the specific policies or procedures called out in Requirement 10, it is equally important to ensure they are properly documented, maintained, and disseminated.
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood. **Customized Approach Objective** Day-to-day responsibilities for performing all the activities in Requirement 10 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.
10.2.1 Audit logs are enabled and active for all system components and cardholder data. **Customized Approach Objective** Records of all activities affecting system components and cardholder data are captured.	Audit logs must exist for all system components. Audit logs send alerts the system administrator, provides data to other monitoring mechanisms, such as intrusion-detection systems (IDS) and security information and event monitoring systems (SIEM) tools, and provide a history trail for post-incident investigation.
10.2.1.1 Audit logs capture all individual user access to cardholder data. **Customized Approach Objective** Records of all individual user access to cardholder data are captured.	It is critical to have a process or system that links user access to system components accessed. Malicious individuals could obtain knowledge of a user account with access to systems in the CDE, or they could create a new,
10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Accounts with increased access privileges, such as the "administrator" or "root" account, have the potential to significantly impact the security or operational functionality of a system. Without a log of the activities

Customized Approach Objective Records of all actions performed by individuals with elevated privileges are captured.	performed, an organization is cannot trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and account.
10.2.1.3 Audit logs capture all access to audit logs. **Customized Approach Objective** Records of all access to audit logs are captured.	Malicious users often attempt to alter audit logs to hide their actions. A record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having logs
10.2.1.4 Audit logs capture all invalid logical access attempts. **Customized Approach Objective** Records of all invalid access attempts are captured.	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password.
10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access. **Customized Approach Objective** Records of all changes to identification and authentication credentials are captured.	Logging changes to authentication credentials (including elevation of privileges, additions, and deletions of accounts with administrative access) provides residual evidence of activities. Malicious users may attempt to manipulate authentication credentials to bypass them or impersonate a valid account.
10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs. **Customized Approach Objective** Records of all changes to audit log activity status are captured.	Turning off or pausing audit logs before performing illicit activities is common practice for malicious users who want to avoid detection. Initialization of audit logs could indicate that that a user disabled the log function to hide their actions.
10.2.1.7 Audit logs capture all creation and deletion of system-level objects. **Customized Approach Objective** Records of alterations that indicate a system has been modified from its intended functionality are captured.	Malicious software, such as malware, often creates or replaces system-level objects on the target system to control a particular function or operation on that system. By logging when system-level objects are created or deleted, it will be easier to determine whether such modifications were authorized.

10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol). **Customized Approach Objective** Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.1 are captured.	By recording these details for the auditable events at 10.2.1.1 through 10.2.1.7, a potential compromise can be quickly identified, with sufficient detail to facilitate following up on suspicious activities.
10.3.1 Read access to audit logs files is limited to those with a job-related need. **Customized Approach Objective** Stored activity records cannot be accessed by unauthorized personnel.	Audit log files contain sensitive information, and read access to the log files must be limited only to those with a valid business need. This access includes audit log files on the originating systems as well as anywhere else they are stored.
10.3.2 Audit log files are protected to prevent modifications by individuals. **Customized Approach Objective** Stored activity records cannot be modified by personnel.	Often a malicious individual who has entered the network will try to edit the audit logs to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a
10.3.3 Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify. **Customized Approach Objective** Stored activity records are secured and preserved in a central location to prevent unauthorized modification.	Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected, even if the system generating the logs becomes compromised.
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts. **Customized Approach Objective** Stored activity records cannot be modified without an alert being generated.	File integrity monitoring or change-detection systems check for changes to critical files and notify when such changes are identified. For file integrity monitoring purposes, an entity usually monitors files that do not regularly change, but when changed, indicate a possible compromise.

10.4.1 The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers). **Customized Approach Objective** Potentially suspicious or anomalous activities are quickly identified to minimize impact.	Many breaches occur months before being detected. Regular log reviews mean incidents can be quickly identified and proactively addressed. Checking logs daily (7 days a week, 365 days a year, including holidays) minimizes the amount of time and exposure of a potential breach. Log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions are examples of automated tools that can be used to meet this requirement.
10.4.1.1 Automated mechanisms are used to perform audit log reviews. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism.	Manual log reviews are difficult to perform, even for one or two systems, due to the amount of log data that is generated. However, using log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions can help facilitate the process by identifying log events that need to be reviewed.
10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically. ***Applicability Notes*** *This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1.* **Customized Approach Objective** Potentially suspicious or anomalous activities for other system components (not included in 10.4.1) are reviewed in accordance with the entity's identified risk.	Periodic review of logs for all other system components (not specified in Requirement 10.4.1) helps to identify indications of potential issues or attempts to access critical systems via less-critical systems.

10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Log reviews for lower-risk system components are performed at a frequency that addresses the entity's risk.	Entities can determine the optimum period to review these logs based on criteria such as the complexity of each entity's environment, the number of types of systems that are required to be evaluated, and the functions of such systems.
10.4.3 Exceptions and anomalies identified during the review process are addressed. **Customized Approach Objective** Suspicious or anomalous activities are addressed.	If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities occurring within their network.
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis. **Customized Approach Objective** Historical records of activity are available immediately to support incident response and are retained for at least 12 months.	Retaining historical audit logs for at least 12 months is necessary because compromises often go unnoticed for significant lengths of time. Having centrally stored log history allows investigators to better determine the length of time a potential breach was occurring, and the possible system(s) impacted. By having three months of logs immediately available, an entity
10.6.1 System clocks and time are synchronized using time-synchronization technology. ***Applicability Notes*** *Keeping time-synchronization technology current includes patching the technology according to PCI DSS Requirement 6.3.1 and 6.3.3.* **Customized Approach Objective** Common time is established across all systems.	Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of events, which is crucial for forensic analysis following a breach.

10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s). **Customized Approach Objective** The time on all systems is accurate and consistent.	Using reputable time servers is a critical component of the time synchronization process. Accepting time updates from specific, industry-accepted external sources helps prevent a malicious individual from changing time settings on systems.
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed. **Customized Approach Objective** System time settings cannot be modified by unauthorized personnel.	Attackers will try to change time configurations to hide their activity. Therefore, restricting the ability to change or modify time synchronization configurations or the system time to administrators will lessen the probability of an attacker successfully changing time configurations.

10.7.1 Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). ***Applicability Notes*** *This requirement will be superseded by Requirement 10.7.2 as of 31 March 2025.*	Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE.
Customized Approach Objective Failures in critical security control systems are promptly identified and addressed.	

10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used). ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment and will supersede Requirement 10.7.1.* **Customized Approach Objective** Failures in critical security control systems are promptly identified and addressed.	Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE.

10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment and will supersede Requirement 10.7.1.*	If alerts from failures of critical security control systems are not responded to quickly and effectively, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment. Documented evidence (for example, records within a problem management system) should provide support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.
Customized Approach Objective Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.	

›nents and Cardholder Data

Control Ownership			Implementation Details	
1800 Notify	Client	Shared	1800 Notify	Client
		X	1800 Notify matains operational procedures that are compliant with PCI DSS	The client must also matain operational procedures that are compliant with PCI DSS
X				
X				
X				
X				

X				
X				
X				
X				
X				
X				

X				
X				
X				
X				
X				

X				
X				
X				

X				
X				
X				
X				

X				
X				

X				

X				

X				

PCI DSS Requirements	Guidance
11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts. ***Applicability Notes*** *The requirement applies even when a policy exists that prohibits the use of wireless technology since attackers do not read and follow company policy.* *Methods used to meet this requirement must be sufficient to detect and identify both authorized and unauthorized devices, including unauthorized devices attached to devices that themselves are authorized.* **Customized Approach Objective** Unauthorized wireless access points are identified and addressed periodically.	Implementation and/or exploitation of wireless technology within a network are common paths for malicious users to gain unauthorized access to the network and cardholder data. Unauthorized wireless devices could be hidden within or attached to a computer or other system component. These devices could also be attached directly to a network port, to a network device such as a switch or router, or inserted as a wireless interface card inside a system component.
11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification. **Customized Approach Objective** Unauthorized wireless access points are not mistaken for authorized wireless access points.	An inventory of authorized wireless access points can help administrators quickly respond when unauthorized wireless access points are detected. This helps to proactively minimize the exposure of CDE to malicious individuals.

11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists. ***Applicability Notes*** *Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a network administrator should not be responsible for scanning the network), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.*	Identifying and addressing vulnerabilities promptly reduces the likelihood of a vulnerability being exploited and the potential compromise of a system component or cardholder data. Vulnerability scans conducted at least every three months provide this detection and identification.
Customized Approach Objective The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.	

11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed. ***Applicability Notes*** *The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Req 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Lower ranked vulnerabilities (lower than high or critical) are addressed at a frequency in accordance with the entity's risk.	All vulnerabilities, regardless of criticality, provide a potential avenue of attack and must therefore be addressed periodically, with the vulnerabilities that expose the most risk addressed more quickly to limit the potential window of attack.

11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • Sufficient privileges are used for those systems that accept credentials for scanning. • If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2. ***Applicability Notes*** *The authenticated scanning tools can be either host-based or network-based.* *"Sufficient" privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities.* *This requirement does not apply to system components that cannot accept credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, and containers.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Automated tools used to detect vulnerabilities can detect vulnerabilities local to each system, which are not visible remotely.	Authenticated scanning provides greater insight into an entity's vulnerability landscape since it can detect vulnerabilities that unauthenticated scans cannot detect. Attackers may leverage vulnerabilities that an entity is unaware of because certain vulnerabilities will only be detected with authenticated scanning. Authenticated scanning can yield significant additional information about an organization's vulnerabilities.

11.3.1.3 Internal vulnerability scans are performed after any significant change as follows: • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). ***Applicability Notes*** *Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed after significant changes.*	Scanning an environment after any significant changes ensures that changes were completed appropriately such that the security of the environment was not compromised because of the change. Entities should perform scans after significant changes as part of the change process per Requirement 6.5.2 and before considering the change complete. All system components affected by the change will need to be scanned.
Customized Approach Objective The security posture of all system components is verified following significant changes to the network or systems, by using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.	

11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan. ***Applicability Notes*** *For initial PCI DSS compliance, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s).* *However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred.* *ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer.* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.* **Customized Approach Objective** This requirement is not eligible for the customized approach.	Attackers routinely look for unpatched or vulnerable externally facing servers, which can be leveraged to launch a directed attack. Organizations must ensure these externally facing devices are regularly scanned for weaknesses and that vulnerabilities are patched or remediated to protect the entity.
11.3.2.1 External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Scanning an environment after any significant changes ensures that changes were completed appropriately such that the security of the environment was not compromised because of the change.

Customized Approach Objective The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.	
11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months. ***Applicability Notes*** *Testing from inside the network (or "internal penetration testing") means testing from both inside the CDE and into the CDE from trusted and untrusted internal networks.* *Testing from outside the network (or "external" penetration testing" means testing the exposed external perimeter of trusted networks, and critical systems connected to or accessible to public network infrastructures.*	Attackers spend a lot of time finding external and internal vulnerabilities to leverage to obtain access to cardholder data and then to exfiltrate that data. As such, entities need to test their networks thoroughly, just as an attacker would do. This testing allows the entity to identify and remediate weakness that might be leveraged to compromise the entity's network and data, and then to take appropriate actions to protect the network and system components from such attacks.

Customized Approach Objective A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker.	
11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology, • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV). **Customized Approach Objective** Internal system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats and ensure that significant changes do not introduce unknown vulnerabilities.	Internal penetration testing serves two purposes. Firstly, just like an external penetration test, it discovers vulnerabilities and misconfigurations that could be used by an attacker that had managed to get some degree of access to the internal network, whether that is because the attacker is an authorized user conducting unauthorized activities, or an external attacker that had managed to penetrate the entity's perimeter. Secondly, internal penetration testing also helps entities to discover where their change control process failed by detecting previously unknown systems. Additionally, it verifies the status of many of the controls operating within the CDE.
11.4.3 External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV). Customized Approach Objective External system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats, and to ensure that significant changes do not introduce unknown vulnerabilities.	A penetration test is not truly a "test" because the outcome of a penetration test is not something that can be classified as a "pass" or a "fail." The best outcome of a test is a catalog of vulnerabilities and misconfigurations that an entity did not know about and the penetration tester found them before an attacker could. A penetration test that found nothing is typically indicative of shortcomings of the penetration tester, rather than being a positive reflection of the security posture of the entity.
11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.	The results of a penetration test are usually a prioritized list of vulnerabilities discovered by the exercise. Often a tester will have chained a number of vulnerabilities together to compromise a system component. Remediating the vulnerabilities found by a penetration test significantly reduces the probability that the same vulnerabilities will be exploited by a

Customized Approach Objective Vulnerabilities and security weaknesses found while verifying system defenses are mitigated.	malicious attacker.
11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	When an entity uses segmentation controls to isolate the CDE from internal untrusted networks, the security of the CDE is dependent on that segmentation functioning. Many attacks have involved the attacker moving laterally from what an entity deemed an isolated network into the CDE. Using penetration testing tools and techniques to validate that an untrusted network is indeed isolated from the CDE can alert the entity to a failure or misconfiguration of the segmentation controls, which can then be rectified.
Customized Approach Objective If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out-of-scope systems.	

11.4.6 Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV). ***Applicability Notes*** *This requirement applies only when the entity being assessed is a service provider.*	Service providers typically have access to greater volumes of cardholder data or can provide an entry point that can be exploited to then compromise multiple other entities. Service providers also typically have larger and more complex networks that are subject to more frequent change. The probability of segmentation controls failing in complex and dynamic networks is greater in service provider environments. Validating segmentation controls more frequently is likely to discover such failings before they can be exploited by an attacker attempting to pivot laterally from an out-of-scope untrusted network to the CDE.
Customized Approach Objective If segmentation is used, it is verified by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.	

11.4.7 Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4. ***Applicability Notes*** *To meet this requirement, third-party hosted/cloud service providers may either:* • *Provide evidence to its customers to show that penetration testing has been performed according to Req 11.4.3 and 11.4.4 on the customers' subscribed infrastructure, or* • *Provide prompt access to each of their customers, so customers can perform their own penetration testing.* *Evidence provided to customers can include redacted penetration testing results but needs to include sufficient information to prove that all elements of Req 11.4.3 and 11.4.4 have been met on the customer's behalf.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken.	Entities need to conduct penetration tests in accordance with PCI DSS to simulate attacker behavior and discover vulnerabilities in their environment. In shared and cloud environments, the multi-tenant service provider may be concerned about the activities of a penetration tester affecting other customers' systems.
11.5.1 Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	Intrusion-detection and/or intrusion-prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and then send alerts and/or stop the attempt as it happens. Without a proactive approach to detect unauthorized activity, attacks on (or misuse of) computer resources could go unnoticed for long periods of time. The impact of an intrusion into the CDE is, in many ways, a factor of the time that an attacker has in the

Customized Approach Objective Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.	CDETs, in many ways, a factor of the time that an attacker has in the environment before being detected.
11.5.1.1 Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Detecting covert malware communication attempts (for example, DNS tunneling) can help block the spread of malware laterally inside a network and the exfiltration of data. When deciding where to place this control, entities should consider critical locations in the network, and likely routes for covert channels.
Customized Approach Objective Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that such communications are blocked.	

11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly. ***Applicability Notes*** *For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change- detection mechanisms such as file integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	Changes to critical system, configuration, or content files can be an indicator an attacker has accessed an organization's system. Such changes can allow an attacker to take additional malicious actions, access cardholder data, and/or conduct activities without detection or record.
Customized Approach Objective Critical files cannot be modified by unauthorized personnel without an alert being generated.	

11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). ***Applicability Notes*** *The intention of this requirement is not that an entity needs to install software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described in the examples above to prevent and detect unexpected script activities.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Many web pages now rely on assembling objects, including active content (primarily JavaScript), from multiple internet locations. Additionally, the content of many web pages is defined using content management and tag management systems that may not be possible to monitor using traditional change detection mechanisms. Therefore, the only place to detect changes or indicators of malicious activity is in the consumer browser as the page is constructed and all JavaScript interpreted.
Customized Approach Objective E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.	

works Regularly

Control Ownership			Implementation Details	
1800 Notify	Client	Shared	1800 Notify	Client
X				
X				

X				

X				

X				

X				

X				
X				

X				
X				

X				
X				
X				

X				

X				

X				
X				

X				

X				

X				

PCI DSS Requirements	Guidance
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners. **Customized Approach Objective** The strategic objectives and principles of information security are defined, adopted, and known to all personnel.	An organization's overall information security policy ties to and governs all other policies and procedures that define protection of cardholder data. The information security policy communicates management's intent and objectives regarding the protection of its most valuable assets, including cardholder data.
12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment. **Customized Approach Objective** The information security policy continues to reflect the organization's strategic objectives and principles.	Security threats and associated protection methods evolve rapidly. Without updating the information security policy to reflect relevant changes, new measures to defend against these threats may not be addressed.
12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities. **Customized Approach Objective** Personnel understand their role in protecting the entity's cardholder data.	Without clearly defined security roles and responsibilities assigned, there could be misuse of the organization's information assets or inconsistent interaction with information security personnel, leading to insecure implementation of technologies or use of outdated or insecure technologies.
12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management. **Customized Approach Objective** A designated member of executive management is responsible for information security.	To ensure someone with sufficient authority and responsibility is actively managing and championing the organization's information security program, accountability and responsibility for information security needs to be assigned at the executive level within an organization.

12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software. ***Applicability Notes*** *Examples of end-user technologies for which acceptable use policies are expected, but are not limited to, remote access and wireless technologies, laptops, tablets, mobile phones, and removable electronic media, email usage, and Internet usage.*	End-user technologies are a significant investment and may pose significant risk to an organization if not managed properly. Acceptable use policies outline the expected behavior from personnel when using the organization's information technology and reflect the organization's risk tolerance.
Customized Approach Objective The use of end-user technologies is defined and managed to ensure authorized usage.	

12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Some PCI DSS requirements allow an entity to define how frequently an activity is performed based on the risk to environment. Performing this risk analysis according to a methodology ensures validity and consistency with policies and procedures. This targeted risk analysis (as opposed to a traditional enterprise-wide risk assessment) focuses on those PCI DSS requirements that allow an entity flexibility about how frequently an entity performs a given control. For this risk analysis, the entity carefully evaluates each PCI DSS requirement that provides this flexibility and determines the frequency that supports adequate security for the entity, and the level of risk the entity is willing to accept.
Customized Approach Objective Up to date knowledge and assessment of risks to the CDE are maintained.	

12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months. ***Applicability Notes*** *This requirement only applies to entities using a Customized Approach.* **Customized Approach Objective** This requirement is part of the customized approach and must be met for those using the customized approach.	A risk analysis following a repeatable and robust methodology enables an entity to meet the customized approach objective. The customized approach to meeting a PCI DSS requirement allows entities to define the controls used to meet a given requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. These controls are expected to at least meet or exceed the security provided by the defined requirement and require extensive documentation by the entity using the customized approach.
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities. ***Applicability Notes*** *The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Protocols and encryption strengths may quickly change or be deprecated due to identification of vulnerabilities or design flaws. In order to support current and future data security needs, entities need to know where cryptography is used and understand how they would be able to respond rapidly to changes impacting the strength of their cryptographic implementations.

Customized Approach Objective The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.	
12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Hardware and software technologies are constantly evolving, and organizations need to be aware of changes to the technologies they use, as well as the evolving threats to those technologies to ensure that they can prepare for, and manage, vulnerabilities in hardware and software that will not be remediated by the vendor or developer.
Customized Approach Objective The entity's hardware and software technologies are up to date and supported by the vendor. Plans to remove or replace all unsupported system components are reviewed periodically.	

12.4.1 Additional requirement for service providers only: Responsibility is established by executive management 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. ***Applicability Notes*** *Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure.* *Responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.*	Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities.
Customized Approach Objective Executives are responsible and accountable for security of cardholder data.	
12.4.2 Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes. ***Applicability Notes*** *This requirement applies only when the entity being assessed is a service provider.*	Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. This requirement is distinct from other requirements that specify a task to be performed. The objective of these reviews is not to reperform other PCI DSS requirements, but to confirm that security activities are being performed on an ongoing basis.

Customized Approach Objective The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.	
12.4.2.1 Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include: • Results of the reviews. • Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program. ***Applicability Notes*** *This requirement applies only when the entity being assessed is a service provider.*	The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, reviews of network security control rulesets—to assist in the entity's preparation for its next PCI DSS assessment.
Customized Approach Objective Findings from operational effectiveness reviews are evaluated by management; appropriate remediation activities are implemented.	
12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	Maintaining a current list of all system components will enable an organization to define the scope of its environment and implement PCI DSS requirements accurately and efficiently. Without an inventory, some system components could be overlooked and be inadvertently excluded
Customized Approach Objective All system components in scope for PCI DSS are identified and known.	

12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. ***Applicability Notes*** *This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the* **Customized Approach Objective** PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures.	Accurate scoping involves critically evaluating the CDE and all connected system components to determine the necessary coverage for PCI DSS requirements. Scoping activities, including careful analysis and ongoing monitoring, help to ensure that in-scope systems are appropriately secured. When documenting account data locations, the entity can consider creating a table or spreadsheet that includes the following information: • Data stores (databases, files, cloud, etc.), including the purpose of data storage and the retention period, • Which CHD elements are stored (PAN, expiry date, cardholder name, and/or any elements of SAD prior to completion of authorization), • How data is secured (type of encryption and strength, hashing algorithm and strength, truncation, tokenization), • How access to data stores is logged, including a description of logging mechanism(s) in use (enterprise solution, application level, operating system level, etc.).

12.5.2.1 Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** The accuracy of PCI DSS scope is verified to be continuously accurate by comprehensive analysis and appropriate technical measures.	Service providers typically have access to greater volumes of cardholder data than do merchants, or can provide an entry point that can be exploited to then compromise multiple other entities. Service providers also typically have larger and more complex networks that are subject to more frequent change. The probability of overlooked changes to scope in complex and dynamic networks is greater in service providers' environments.
12.5.3 Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** PCI DSS scope is confirmed after significant organizational change.	An organization's structure and management define the requirements and protocol for effective and secure operations. Changes to this structure could have negative effects to existing controls and frameworks by reallocating or removing resources that once supported PCI DSS controls or inheriting new responsibilities that may not have established controls in place. Therefore, it is important to revisit PCI DSS scope and controls when there are changes to an organization's structure and management to ensure controls are in place and active.
12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data. **Customized Approach Objective** Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.	If personnel are not educated about their company's information security policies and procedures and their own security responsibilities, security safeguards and processes that have been implemented may become ineffective through unintentional errors or intentional actions.

12.6.2 The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** The content of security awareness material is reviewed and updated periodically.	The threat environment and an entity's defenses are not static. As such, the security awareness program materials must be updated as frequently as needed to ensure that the education received by personnel is up to date and represents the current threat environment.
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures. **Customized Approach Objective** Personnel remain knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.	Training of personnel ensures they receive the information about the importance of information security and that they understand their role in protecting the organization. Requiring an acknowledgment by personnel helps ensure that they have read and understood the security policies and procedures, and that they have made and will continue to make a commitment to comply with these policies.

12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks. • Social engineering. ***Applicability Notes*** *See Requirement 5.4.1 for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one.* *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.	Educating personnel on how to detect, react to, and report potential phishing and related attacks and social engineering attempts is essential to minimizing the probability of successful attacks.
12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Personnel are knowledgeable about their responsibility for the security and operation of end-user technologies and are able to access assistance and guidance when required.	By including the key points of the acceptable use policy in regular training and the related context, personnel will understand their responsibilities and how these impact the security of an organization's systems.

12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources. ***Applicability Notes*** *For those potential personnel to be hired for positions such as store cashiers, who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.* **Customized Approach Objective** The risk related to allowing new members of staff access to the CDE is understood and managed.	Performing thorough screening prior to hiring potential personnel who are expected to be given access to the CDE provides entities with the information necessary to make informed risk decisions regarding personnel they hire that will have access to the CDE.
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided. ***Applicability Notes*** *The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.* **Customized Approach Objective** Records are maintained of TPSPs and the services provided.	Maintaining a list of all TPSPs identifies where potential risk extends outside the organization and defines the organization's extended attack surface.

12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE. ***Applicability Notes*** *The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement.* *Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) or a declaration on a company's website) is not the same as a written agreement specified in this requirement.* **Customized Approach Objective** Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.	The written acknowledgment from a TPSP demonstrates its commitment to maintaining proper security of account data that it obtains from its customers and that the TPSP is fully aware of the assets that could be affected during the provisioning of the TPSP's service. The extent to which a specific TPSP is responsible for the security of account data will depend on the service provided and the agreement between the provider and assessed entity (the customer).
12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement. **Customized Approach Objective** The capability, intent, and resources of a prospective TPSP to adequately protect account data are assessed before the TPSP is engaged.	A thorough process for engaging TPSPs, including details for selection and vetting prior to engagement, helps ensure that a TPSP is thoroughly vetted internally by an entity prior to establishing a formal relationship and that the risk to cardholder data associated with the engagement of the TPSP is understood.

12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months. ***Applicability Notes*** *Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.* **Customized Approach Objective** The PCI DSS compliance status of TPSPs is verified periodically.	Knowing the PCI DSS compliance status of all engaged TPSPs provides assurance and awareness about whether they comply with the requirements applicable to the services they offer to the organization.
12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity. **Customized Approach Objective** Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.	It is important that the entity understands which PCI DSS requirements and sub-requirements its TPSPs have agreed to meet, which requirements are shared between the TPSP and the entity, and for those that are shared, specifics about how the requirements are shared and which entity is responsible for meeting each sub-requirement.
12.9.1 Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP 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 CDE. ***Applicability Notes*** *The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement.*	In conjunction with Requirement 12.8.2, this requirement is intended to promote a consistent level of understanding between TPSPs and their customers about their applicable PCI DSS responsibilities. The acknowledgment of the TPSPs evidences their commitment to maintaining proper security of account data that it obtains from its clients. The method by which the TPSP provides written acknowledgment should be agreed between the provider and its customers.

Customized Approach Objective TPSPs formally acknowledge their security responsibilities to their customers.	
12.9.2 Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5). ***Applicability Notes*** *This requirement applies only when the entity being assessed is a service provider.*	If a TPSP does not provide the necessary information to enable its customers to meet their security and compliance requirements, the customers will not be able to protect cardholder data nor meet their own contractual obligations. If a TPSP has a PCI DSS Attestation of Compliance (AOC), the expectation is that the TPSP should provide that to customers upon request to demonstrate their PCI DSS compliance status.
Customized Approach Objective TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.	
12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • 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.	Without a comprehensive incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as risk of financial and/or reputational loss and legal liabilities.

Customized Approach Objective A comprehensive incident response plan that meets card brand expectations is maintained.	
12.10.2 At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1. **Customized Approach Objective** The incident response plan is kept current and tested periodically.	Proper testing of the security incident response plan can identify broken business processes and ensure key steps are not missed, which could result in increased exposure during an incident. Periodic testing of the plan ensures that the processes remain viable, as well as ensuring that all relevant personnel in the organization are familiar with the plan.
12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents. **Customized Approach Objective** Incidents are responded to immediately where appropriate.	An incident could occur at any time, therefore if a person who is trained in incident response and familiar with the entity's plan is available when an incident is detected, the entity's ability to correctly respond to the incident is increased.
12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities. **Customized Approach Objective** Personnel are knowledgeable about their role and responsibilities in incident response and are able to access assistance and guidance when required.	Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become "polluted" by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation.
12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Incident response personnel are trained at a frequency that addresses the entity's risk.	Each entity's environment and incident response plan are different and the approach will depend on a number of factors, including the size and complexity of the entity, the degree of change in the environment, the size of the incident response team, and the turnover in personnel.

12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • Detection of unauthorized wireless access points. • The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. ***Applicability Notes*** *The bullet above (for monitoring and responding to alerts from a change- and tamper-detection mechanism for payment pages) is a best practice until 31 March 2025, after which it will be required as part of Req 12.10.5 and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.	Responding to alerts generated by security monitoring systems that are explicitly designed to focus on potential risk to data is critical to prevent a breach and therefore, this must be included in the incident-response processes.
12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments. **Customized Approach Objective** The effectiveness and accuracy of the incident response plan is reviewed and updated after each invocation.	Incorporating lessons learned into the incident response plan after an incident occurs and in-step with industry developments, helps keep the plan current and able to react to emerging threats and security trends.

12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected. ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Having documented incident response procedures that are followed in the event that stored PAN is found anywhere it is not expected to be, helps to identify the necessary remediation actions and prevent future leaks. If PAN was found outside the CDE, analysis should be performed to 1) determine whether it was saved independently of other data or with sensitive authentication data, 2) identify the source of the data, and 3) identify the control gaps that resulted in the data being outside the CDE.
Customized Approach Objective Processes are in place to quickly respond, analyze, and address situations in the event that cleartext PAN is detected where it is not expected.	

ational Policies and Programs

Control Ownership			Implementation Details	
1800 Notify	Client	Shared	1800 Notify	Client
		X	1800 Notify matains an information security policy that is compliant with PCI DSS	The client must also matain an information security policy that is compliant with PCI DSS
X				
X				
X				

X				

X				

X				
X				

X				

X				
X				

X				
X				

X				

X				
X				
X				

X				
X				

X				
X				

X				
X				

X				
X				

X				
X				
X				

X				
X				

X				
X				
X				
X				

X				
X				

X				

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers
PCI DSS Requirements
A1.1.1 Defined Approach Requirements Logical separation is implemented as follows: • The provider cannot access its customers' environments without authorization • Customers cannot access the provider's environment without authorization ***Applicability Notes*** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* **Customized Approach Objective** Customers cannot access the provider's environment. The provider cannot access its customers' environments without authorization.

A1.1.2 Defined Approach Requirements
Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.

Customized Approach Objective
Customers cannot access other customers' environments.

A1.1.3 Defined Approach Requirements
Controls are implemented such that each customer can only access resources allocated to them.

Customized Approach Objective
Customers cannot impact resources allocated to other customers.

A1.1.4 Defined Approach Requirements
The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.

Applicability Notes
The testing of adequate separation between customers in a multi-tenant service provider environment is in addition to the penetration tests specified in Req 11.4.6.
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment

Customized Approach Objective
Segmentation of customer environments from other environments is periodically validated to be effective.

A1.2.1 Defined Approach Requirements

Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including:

- Logs are enabled for common third-party applications
- Logs are active by default
- Logs are available for review only by the owning customer
- Log locations are clearly communicated to the owning customer
- Log data and availability is consistent with PCI DSS Req 10

Customized Approach Objective

Log capability is available to all customer without affecting the confidentiality of other customers.

A1.2.2 Defined Approach Requirements

Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer.

Customized Approach Objective

Forensic investigation is readily available to all customers in the event of a suspected or confirmed security incident.

A1.2.3 Defined Approach Requirements

Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including:

• Customers can securely report security incidents and vulnerabilities to the provider

• The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Req 6.3.1

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Customized Approach Objective

Suspected or confirmed security incidents or vulnerabilities are discovered and addressed. Customers are informed where appropriate.

Guidance	Control Ownership			Implementat
	TPSP	Client	Shared	TPSP
Purpose Without controls between the provider's environment and the customer's environment, a malicious actor within the provider's environment could compromise the customer's environment, and similarly, a malicious actor in a customer environment could compromise the provider and potentially other of the provider's customers. Multi-tenant environments should be isolated from each other and from the provider's infrastructure such that they can be separately managed entities with no connectivity between them. **Good Practice** Providers should ensure strong separation between the environments that are designed for customer access, for example, configuration and billing portals, and the provider's private environment that should only be accessed by authorized provider personnel. Service provider access to customer environments is performed in accordance with Req 8.2.3. **Further Information** Refer to the Information Supplement: PCI SSC Cloud Computing Guidelines for further guidance on cloud environments.				NOT APPLICABLE FOR 1800 NOTIFY

Purpose It is important that a multi-tenant service provider define controls so that each customer can only access their own environment and CDE to prevent unauthorized access from one customer's environment to another. **Examples** In a cloud-based infrastructure, such as an infrastructure as a service (IaaS) offering, the customers' CDE may include virtual network devices and virtual servers that are configured and managed by the customers, including operating systems, files, memory, etc.				NOT APPLICABLE FOR 1800 NOTIFY
Purpose To prevent any inadvertent or intentional impact to other customers' environments or account data, it is important that each customer can access only resources allocated to that customer.				NOT APPLICABLE FOR 1800 NOTIFY
Purpose Multi-tenant services providers are responsible for managing the segmentation between their customers. Without technical assurance that segmentation controls are effective, it is possible that changes to the service provider's technology would inadvertently create a vulnerability that could be exploited across all the service provider's customers. **Good Practice** Effectiveness of separation techniques can be confirmed by using service-provider-created temporary (mock-up) environments that represent customer environments and attempting to 1) access one temporary environment from another environment, and 2) access a temporary environment from the Internet.				NOT APPLICABLE FOR 1800 NOTIFY

Purpose Log information is useful for detecting and troubleshooting security incidents and is invaluable for forensic investigations. Customers therefore need to have access to these logs. However, log information can also be used by an attacker for reconnaissance, and so a customer's log information must only be accessible by the customer that the log relates to.				NOT APPLICABLE FOR 1800 NOTIFY
Purpose In the event of a suspected or confirmed breach of confidentiality of cardholder data, a customer's forensic investigator aims to find the cause of the breach, exclude the attacker from the environment, and ensure all unauthorized access is removed. Prompt and efficient responses to forensic investigators' requests can significantly reduce the time taken for the investigator to secure the customer's environment.				NOT APPLICABLE FOR 1800 NOTIFY

Purpose Security vulnerabilities in the provided services can impact the security of all the service provider's customers and therefore must be managed in accordance with the service provider's established processes, with priority given to resolving vulnerabilities that have the highest probability of compromise. Customers are likely to notice vulnerabilities and security misconfigurations while using the service. Implementing secure methods for customers to report security incidents and vulnerabilities encourages customers to report potential issues and enable the provider to quickly learn about and address potential issues within their environment.				NOT APPLICABLE FOR 1800 NOTIFY