

# THE GUIDE TO PCI DSS

## 3.2



# TABLE OF CONTENTS


<u><a href="#">PCI DSS V3.2: WHAT YOU NEED TO KNOW .....</a></u>	<u><a href="#">3</a></u>
<u><a href="#">Introduction to PCI DSS 3.2.....</a></u>	<u><a href="#">3</a></u>
<u><a href="#">General Changes and Clarifications.....</a></u>	<u><a href="#">3</a></u>
<u><a href="#">SSL and Early TLS Risk Mitigation/Migration Plan .....</a></u>	<u><a href="#">17</a></u>
<u><a href="#">Significant Changes &amp; Multi-factor Authentication Changes.....</a></u>	<u><a href="#">18</a></u>
<u><a href="#">Changes for Service Providers.....</a></u>	<u><a href="#">20</a></u>
<u><a href="#">References and Resources .....</a></u>	<u><a href="#">23</a></u>

# PCI DSS V3.2: WHAT YOU NEED TO KNOW

## INTRODUCTION TO PCI DSS 3.2

On April 16, 2016, the Payment Card Industry (PCI) Data Security Standard (DSS) version 3.2 was published, and with it came many changes for both merchants and service providers. As always, the Security Standards Council (SSC) has given time for entities to comply with the new requirements, which became mandatory as of October 2016. For evolving requirements, entities have been given until February of 2018 to comply with the more rigorous requirements that were introduced with this version of the DSS.

Aside from the changes to the security standard's requirements, the SSC has decided to make a shift of their revision process. With the PCI DSS now being considered a "mature standard" the SSC will no longer be utilizing a three-year revision cycle. Instead, they will be taking a more iterative approach which means more publications with fewer changes. Version 3.2 is the beginning of this paradigm shift.

 *PCI validations, may be a point-in-time assessment, but merchants and service providers are required to maintain compliance throughout the year*

The most significant changes brought on by this new version of the DSS include **changes to multi-factor authentication** and **more stringent requirements for service providers**. However, one of the subtler changes is an increased emphasis on PCI compliance as a business-as-usual (BAU) practice. PCI validations, may be a point-in-time assessment, but merchants and service providers are required to maintain compliance throughout the year and should be able to provide documented evidence of these BAU activities. These changes will be discussed in further detail below.

## GENERAL CHANGES AND CLARIFICATIONS

Throughout the PCI DSS, minor typographical errors and readability improvements were addressed; additionally, the language and/or testing procedures for many requirements were updated for consistency. Within the introduction, changes were made to clarify that security threats are always evolving and PA-DSS applications that are no longer supported by the vendor may not offer the same level of security as supported versions. It was also clarified that backup/recovery sites need to be considered when addressing the scope of PCI DSS requirements. Also, all examples of strong or secure protocol/encryption types have been removed from the standard. As seen in the past with SSL and early TLS, what is considered to be a strong or secure protocol can change overnight. Entities still undergoing a SSL early TLS migration are now required to document their migration process in the new Appendix A2 section. Along with the addition of Appendix A2, the SSC has added Appendix A3 which is to be used for designated entities which are defined as "entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements."

# GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
All	All	Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.	
<b>Relationship between PCI DSS and PA-DSS</b>	Relationship between PCI DSS and PA-DSS	Added guidance that security threats are constantly evolving, and payment applications that are not supported by the vendor may not offer the same level of security as supported version.	The PA-DSS requirements are derived from the PCI DSS Requirements and Security Assessment Procedures. The PA-DSS details the requirements a payment application must meet in order to facilitate a customer's PCI DSS compliance. <b>As security threats are constantly evolving, applications that are no longer supported by the vendor (e.g., identified by the vendor as "end of life") may not offer the same level of security as supported versions.</b>
<b>Scope of PCI DSS Requirements</b>	Scope of PCI DSS Requirements	Clarified that backup/recovery sites need to be considered when confirming PCI DSS scope.	The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in the PCI DSS scope. <b>All types of systems and locations should be considered as part of the scoping process, including backup/recovery sites and failover systems.</b>

# GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
<b>Best Practices for Implementing PCI DSS into Business-as-Usual Processes</b>	Best Practices for Implementing PCI DSS into Business-as-Usual Processes	Updated Note to clarify that some business-as-usual principles may be requirements for certain entities, such as those defined in the Designated Entities Supplemental Validation (Appendix A3).	
	PCI DSS Versions	New section to describe how this version of PCI DSS impacts the previously-effective version.	
<b>General</b>	General	Removed examples of “strong” or “secure” protocols from a number of requirements, as these may change at any time.	
<b>General</b>	General	Moved examples from a number of requirements and/or testing procedures to the Guidance column, and added guidance where appropriate.	
<b>General</b>	General	Changed “passwords/phrases” to “passwords/passphrases” in a number of requirements for consistency.	

# GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
General	General	Clarified correct term is multi-factor authentication, rather than two-factor authentication, as two or more factors may be used.	
General	General	Removed notes from requirements referring to an effective date of July 1, 2015, as these are now effective. Affected requirements are 6.5.10, 8.5.1, 9.9, 11.3, and 12.9.	
1.1.6	1.1.6	Clarified that approval of business use is included in the justification. Removed examples of “insecure” protocols as these may change in accordance with industry standards.	Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.
1.2.1	1.2.1	Added guidance to clarify intent of requirement.	<b>Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, thus preventing unfiltered access between untrusted and trusted environments.</b> This prevents malicious individuals from accessing the entity’s network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within the entity’s network out to an untrusted server). Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.

## GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
1.3	1.3	Added guidance to clarify intent of requirement.	<b>While there may be legitimate reasons for untrusted connections to be permitted to DMZ systems (e.g., to allow public access to a web server), such connections should never be granted to systems in the internal network.</b> A firewall's intent is to manage and control all connections between public systems and internal systems, especially those that store, process or transmit cardholder data. If direct access is allowed between public systems and the CDE, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.
1.3.3	N/A	Removed requirement as intent is addressed via other requirements in 1.2 and 1.3	N/A
1.3.4 – 1.3.8	1.3.4 – 1.3.8	Renumbered due to removal of former Requirement 1.3.3.	N/A
1.3.6	1.3.5	Updated to clarify intent of requirement rather than use of a particular type of technology.	Permit only "established" connections into the network.

# GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
1.4	1.4	Increased flexibility by including or equivalent functionality as alternative to personal firewall software. Clarified requirement applies to all portable computing devices that connect to the Internet when outside the network and that also access the CDE.	<p><b>Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned)</b> that connect to the Internet when outside the network (for example, laptops used by employees), <b>and which are also used to access the CDE.</b> Firewall <b>(or equivalent)</b> configurations include:</p> <ul style="list-style-type: none"> <li>• Specific configuration settings are defined.</li> <li>• Personal firewall <b>(or equivalent functionality)</b> is actively running.</li> <li>• Personal firewall <b>(or equivalent functionality)</b> is not alterable by users of the portable computing devices</li> </ul>
2.1	2.1	Clarified requirement applies to payment applications.	<p><b>Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.</b></p> <p>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, <b>payment applications</b>, Simple Network Management Protocol (SNMP) community strings, etc.).</p>
2.2.3	2.2.3	Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2.	<p>Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.</p> <p>Note: <b>Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.</b></p>



# GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
2.3	2.3	Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2. Removed reference to “web-based management” as requirement already specifies “all non-console administrative access”, which by definition includes any web- based access.	<p>Encrypt all non-console administrative access using strong cryptography.</p> <p>Note: <b>Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.</b></p>
3.3	3.3	Updated requirement to clarify that any displays of PAN greater than the first six/last four digits of the PAN requires a legitimate business need. Added guidance on common masking scenarios.	<p>The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that full PAN is only displayed for those with a legitimate business need to see the full PAN minimizes the risk of unauthorized persons gaining access to PAN data.</p> <p><b>The masking approach should always ensure that only the minimum number of digits is displayed as necessary to perform a specific business function. For example, if only the last four digits are needed to perform a business function, mask the PAN so that individuals performing that function can view only the last four digits. As another example, if a function needs access to the bank identification number (BIN) for routing purposes, unmask only the BIN digits (traditionally the first six digits) during that function. This requirement relates to protection of PAN displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.4 for protection of PAN when stored in files, databases, etc.</b></p>

## GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
3.4.d	3.4.d	Updated testing procedure to clarify the examination of audit logs includes payment application logs	Examine a sample of audit logs, <b>including payment application logs</b> , to confirm that PAN is rendered unreadable <b>or is not present in the logs</b> .
3.4.1	3.4.1	Added note to requirement to clarify the requirement applies in addition to all other PCI DSS encryption and key management requirements.	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. Note: <b>This requirement applies in addition to all other PCI DSS encryption and key management requirements.</b>
3.6.1.b	3.6.1.b	Updated testing procedure language to clarify testing involves observation of procedures rather than key-generation method itself, as this should not be observable. Added guidance referring to Glossary definition for “Cryptographic Key Generation”	Observe the <b>procedures</b> for generating keys to verify that strong keys are generated.

# GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
4.1	4.1	Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2.	<p>Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:</p> <ul style="list-style-type: none"> <li>• Only trusted keys and certificates are accepted.</li> <li>• The protocol in use only supports secure versions or configurations.</li> <li>• The encryption strength is appropriate for the encryption methodology in use.</li> </ul> <p>Note: <b>Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.</b></p> <p>Examples of open, public networks include but are not limited to:</p> <ul style="list-style-type: none"> <li>• <b>The Internet</b></li> <li>• <b>Wireless technologies, including 802.11 and Bluetooth</b></li> <li>• <b>Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)</b></li> <li>• <b>General Packet Radio Service (GPRS)</b></li> <li>• <b>Satellite communications</b></li> </ul>

## GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
6.2	6.2	Added clarification to Guidance column that requirement to patch all software includes payment applications.	<p>There is a constant stream of attacks using widely published exploits, often called “zero day” (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. If the most recent patches are not implemented on critical systems as soon as possible, a malicious individual can use these exploits to attack or disable a system, or gain access to sensitive data.</p> <p>Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months. <b>This requirement applies to applicable patches for all installed software, including payment applications (both those that are PA-DSS validated and those that are not).</b></p>
6.4.4	6.4.4	Updated requirement to align with testing procedure.	Removal of test data and accounts from system components <b>before the system becomes active / goes into production.</b>
6.4.5	6.4.5	Clarified that change control processes are not limited to patches and software modifications.	<p><b>Examine documented change control procedures and verify procedures are defined for:</b></p> <ul style="list-style-type: none"> <li>• Documentation of impact</li> <li>• Documented change approval by authorized parties</li> <li>• Functionality testing to verify that the change does not adversely impact the security of the system</li> <li>• Back-out procedures</li> </ul>

# GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
6.5	6.5	Clarified that training for developers must be up to date and occur at least annually.	Address common coding vulnerabilities in software-development processes as follows: <ul style="list-style-type: none"> <li>• Train developers <b>at least annually in up-to-date secure coding techniques</b>, including how to avoid common coding vulnerabilities.</li> <li>• Develop applications based on secure coding guidelines.</li> </ul>
<b>6.5.a – 6.5.d</b>	6.5.a – 6.5.d	Removed Testing Procedure 6.5.b and renumbered remaining testing	N/A
7.2	7.2	Updated requirement, testing procedures and Guidance column to clarify that one or more access control systems may be used.	Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed. This access control system(s) must include the following:
<b>Requirement 8</b>	Requirement 8	Added note to Requirement 8 introduction that the authentication requirements do not apply to accounts used by consumers (e.g. cardholders).	Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance). <b>These requirements do not apply to accounts used by consumers (e.g., cardholders).</b>
8.1.5	8.1.5	Clarified requirement intended for all third parties with remote access, rather than only vendors.	Manage IDs used by <b>third parties to access</b> , support, or maintain system components via remote access as follows: <ul style="list-style-type: none"> <li>• Enabled only during the time period needed and disabled when not in use.</li> <li>• Monitored when in use.</li> </ul>

# GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
8.2.3	8.2.3	Updated Guidance column to reflect changing industry standards.	<p>Strong passwords/passphrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or nonexistent passwords. If passwords are short or simple to guess, 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. This requirement specifies that a minimum of seven characters and both numeric and alphabetic characters should be used for passwords/ <b>passphrases</b>. For cases where this minimum cannot be met due to technical limitations, entities can use “equivalent strength” to evaluate their alternative.</p> <p><b>For information on variability and equivalency of password strength (also referred to as entropy) for passwords/passphrases of different formats, refer to industry standards (e.g., the current version of NIST SP 800-63.)</b></p> <p>Note: Testing Procedure 8.2.3.b is an additional procedure that only applies if the entity being assessed is a service provider</p>
8.3	8.3	Clarified correct term is multi-factor authentication rather than two-factor authentication, as two or more factors may be used.	Secure all individual non-console administrative access and all remote access to the CDE using <b>multi-factor</b> authentication.
9.1.1	9.1.1	Clarified that either video cameras or access controls mechanisms, or both, may be used.	Use either <b>video cameras or access control mechanisms (or both)</b> to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.
9.5.1.a – 9.5.1.b	9.5.1.a – 9.5.1.b	Combined testing procedures to clarify that assessor verifies the storage location is reviewed at least annually.	N/A

## GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
10.8	10.8	Renumbered due to addition of new Requirement 10.8.	N/A
11.2.1	11.2.1	Clarified that all “high risk” vulnerabilities must be addressed in accordance with the entity’s vulnerability ranking (as defined in Requirement 6.1), and verified by rescans.	Perform quarterly internal vulnerability scans. <b>Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking</b> (per Requirement 6.1). Scans must be performed by qualified personnel.
11.3.4	11.3.4	Added Testing Procedure 11.3.4.c to confirm penetration test is performed by a qualified internal resource or qualified external third party.	<b>Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).</b>
11.5.a	11.5.a	Removed “within the cardholder data environment” from testing procedure for consistency with requirement, as requirement may apply to critical systems located outside the designated CDE.	Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: <ul style="list-style-type: none"> <li>• System executables</li> <li>• Application executables</li> <li>• Configuration and parameter files</li> <li>• Centrally stored, historical or archived, log and audit files</li> <li>• Additional critical files determined by entity (for example, through risk assessment or other means).</li> </ul>
12.3.3	12.3.3	Reformatted testing procedure for clarity.	12.3.3 Verify that the usage policies define: <ul style="list-style-type: none"> <li>• <b>A list of all critical devices, and</b></li> <li>• <b>A list of personnel authorized to use the devices</b></li> </ul>

## GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
12.4	12.4.1	Renumbered due to addition of new Requirement 12.4.	N/A
12.6	12.6	Clarified intent of security awareness program is to ensure personnel are aware of the cardholder data security policy and procedures.	Implement a formal security awareness program to make <b>all personnel aware of the cardholder data security policy and procedures.</b>
12.8.1	12.8.1	Clarified that the list of service providers includes a description of the service provided.	Maintain a list of service providers <b>including a description of the service provided.</b>
12.8.2	12.8.2	Added guidance that service provider responsibility will depend on the particular service being provided and the agreement between the two parties.	The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. <b>The extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity.</b> In conjunction with Requirement 12.9, <b>this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities.</b> For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service.
12.10.2	12.10.2	Clarified that review of the incident response plan encompasses all elements listed in Requirement 12.10.1.	Interview personnel and review documentation from testing to verify that the plan is tested at least annually, <b>and that testing includes all elements listed in Requirement 12.10.1.</b>
Appendix A	Appendix A	Renumbered Appendix “Additional PCI DSS Requirements for Shared Hosting Providers” due to inclusion of new appendices.	N/A



## GENERAL CHANGES

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT all bold text is new or updated
<b>Appendix A2</b>	Appendix A2	New Appendix with additional requirements for entities using SSL/early TLS, incorporating new migration deadlines for removal of SSL/early TLS	N/A
<b>Appendix A2</b>	Appendix A2	New Appendix to incorporate the “Designated Entities Supplemental Validation” (DESV), which was previously a separate document.	N/A

### SSL AND EARLY TLS RISK MITIGATION/MIGRATION PLAN

As previously mentioned, Appendix A2 requires that any entity with SSL or early TLS implementations still within their cardholder data environment (CDE) must have a formal plan in place to migrate to a secure version of TLS, and a plan to mitigate the risk posed by any vulnerabilities that have been exposed in these protocols. If either SSL or early TLS is still in use on any device, including POI/POS terminals, the Risk Mitigation and Migration Plan will need to be documented and used as evidence to meet PCI DSS compliance requirements. The SSL and early TLS requirements have not changed since version 3.1 of the PCI DSS, they were simply moved to Appendix A2.

All organizations are expected to be migrated off SSL and early TLS by **June 30, 2018**.

# SIGNIFICANT/EVOLVING REQUIREMENTS:

## SIGNIFICANT/EVOLVING REQUIREMENTS

Version 3.2 of the DSS brings significant changes to how multi-factor authentication is to be implemented and new requirements that service providers must adhere to. Trends have shown that many CDE breaches have originated from out of scope systems which was the catalyst for expanding on requirement 8.3 to improve perimeter defenses through strict multi-factor authentication. This includes requiring multi-factor authentication for any non-console, remote, or administrative access into the CDE. Also included are the many new requirements that service providers must adhere to; as well as an additional change control process for all entities. While all evolving requirements remain best practice until February 2018, it is highly recommended that organizations take immediate steps to begin implementation.

## MULTI-FACTOR AUTHENTICATION CHANGES

As mentioned, some of the more significant changes to the DSS in version 3.2 were made to multi-factor authentication. In the past, two-factor authentication was only required for individuals accessing components from outside the network. However, as trends were analyzed, the council realized that many breaches originated from outside of the CDE. This prompted the expansion of dual-factor authentication from one, to three requirements (8.3, 8.3.1, & 8.3.2). Now, not only is multi-factor authentication required for remote network access for all users (admin, user, and third-party), but as an additional barrier, multi-factor may be required to enter the CDE from within the corporate network.

To further explain the changes and council's stance on secure implementations of multi-factor authentication, the PCI SSC released additional guidance for multi-factor authentication requirements. The documentation explains that multi-factor authentication is only secure if the factors of authentication are independent of one another. For example, if an administrator were to use a laptop which had a software based certificate stored on it and required the same login credentials to unlock as the component in the CDE, this would not be considered independent. There are other instances where an organization may utilize an application to generate a one-time password as the second form of authentication. If this application were to reside on the same device as the one used to gain access to the CDE, the factors would not be considered independent. The council's goal here is to prevent a device from being a single point of failure were an attacker to gain control of it. While SMS communication of an authentication factor is currently allowed, NIST has advised that the security of this method has depreciated and further releases may not allow for such activity.

Please reference the following table to quickly view these requirements.

## SIGNIFICANT/EVOLVING REQUIREMENTS:

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT
	6.4.6	New requirement for change control processes to include verification of PCI DSS requirements impacted by a change. <b>Effective February 1, 2018</b>	<p>Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.</p> <p>Note: This requirement is a best practice <b>until January 31, 2018</b>, after which it becomes a requirement.</p>
<b>8.3</b>	8.3, 8.3.1, 8.3.2	Expanded Requirement 8.3 into sub-requirements, to require multi-factor authentication for all personnel with non-console administrative access, and all personnel with remote access to the CDE.	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.
	8.3.1	New Requirement 8.3.1 addresses multi-factor authentication for all personnel with non-console administrative access to the CDE. Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. Requirement 8.3.1 <b>effective February 1, 2018</b>	<p>Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.</p> <p>Note: This requirement is a best practice <b>until January 31, 2018</b>, after which it becomes a requirement.</p>
	8.3.2	New Requirement 8.3.2 addresses multi-factor authentication for all personnel with remote access to the CDE (incorporates former Requirement 8.3).	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.

# NEW SERVICE PROVIDER REQUIREMENTS:

## CHANGES FOR SERVICE PROVIDERS

As there has been a trend in breaches originating from Service Providers, the PCI SSC has reacted and added additional requirements that service providers must adhere to. All new service provider related controls are a **best practice until January 31, 2018** after which, they will become a requirement. Additional security controls for service providers include requiring that cryptographic architecture documentation is maintained, detecting and reporting any failures of critical security systems, performing penetration tests on segmentation every six months, establishing PCI responsibilities for executive management and performing quarterly reviews to ensure personnel are following security policies and operational procedures. All of these newly added requirements stem from the SSC's efforts to make PCI a part of daily BAU activities.

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT
	3.5.1	New requirement for service providers to maintain a documented description of the cryptographic architecture. <b>Effective February 1, 2018</b>	Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: <ul style="list-style-type: none"> <li>• Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date</li> <li>• Description of the key usage for each key</li> <li>• Inventory of any HSMs and other SCDs used for key management</li> </ul>
	10.8	New requirement for service providers to detect and report on failures of critical security control systems. <b>Effective February 1, 2018</b>	<i>Additional requirement for service providers only:</i> Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Anti-virus</li> <li>• Physical access controls</li> <li>• Logical access controls</li> <li>• Audit logging mechanisms</li> <li>• Segmentation controls (if used)</li> </ul>

*Note:* This requirement is a best practice **until January 31, 2018**, after which it becomes a requirement.

## NEW SERVICE PROVIDER REQUIREMENTS:

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT
	10.8.1	<p>New requirement for service providers to detect and report on failures of critical security control systems.</p> <p><b>Effective February 1, 2018</b></p>	<p><i>Additional requirement for service providers only:</i> Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:</p> <ul style="list-style-type: none"> <li>• Restoring security functions</li> <li>• Identifying and documenting the duration (date and time start to end) of the security failure</li> <li>• Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause</li> <li>• Identifying and addressing any security issues that arose during the failure</li> <li>• Performing a risk assessment to determine whether further actions are required as a result of the security failure</li> <li>• Implementing controls to prevent cause of failure from reoccurring</li> <li>• Resuming monitoring of security controls</li> </ul> <p><i>Note:</i> This requirement is a best practice <b>until January 31, 2018</b>, after which it becomes a requirement.</p>
	11.3.4.1	<p>New requirement for service providers to perform penetration testing on segmentation controls at least every six months.</p> <p><b>Effective February 1, 2018</b></p>	<p><i>Additional requirement for service providers only:</i> If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.</p> <p><i>Note:</i> This requirement is a best practice <b>until January 31, 2018</b>, after which it becomes a requirement.</p>

## NEW SERVICE PROVIDER REQUIREMENTS:

PCI DSS V3.1	PCI DSS V3.2	CHANGE	UPDATED TEXT
	12.4.1	<p>New requirement for service providers' executive management to establish responsibilities for the protection of cardholder data and a PCI DSS compliance program.</p> <p><b>Effective February 1, 2018</b></p>	<p><i>Additional requirement for service providers only:</i> Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:</p> <ul style="list-style-type: none"> <li>• Overall accountability for maintaining PCI DSS compliance</li> <li>• Defining a charter for a PCI DSS compliance program</li> </ul> <p><i>Note:</i> This requirement is a best practice <b>until January 31, 2018</b>, after</p>
	12.11	<p>New requirement for service providers to perform reviews at least quarterly, to confirm personnel are following security policies and operational procedures.</p> <p><b>Effective February 1, 2018</b></p>	<p><i>Additional requirement for service providers only:</i> Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:</p> <ul style="list-style-type: none"> <li>• Daily log reviews</li> <li>• Firewall rule-set reviews</li> <li>• Applying configuration standards to new systems</li> <li>• Responding to security alerts</li> <li>• Change management processes</li> </ul> <p><i>Note:</i> This requirement is a best practice <b>until January 31, 2018</b>, after which it becomes a requirement.</p>
	12.11.1	<p>New requirement for service providers to perform reviews at least quarterly, to confirm personnel are following security policies and operational procedures.</p> <p><b>Effective February 1, 2018</b></p>	<p><i>Additional requirement for service providers only:</i> Maintain documentation of quarterly review process to include:</p> <ul style="list-style-type: none"> <li>• Documenting results of the reviews</li> <li>• Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program</li> </ul>

## REFERENCES AND RESOURCES

Multi-Factor Authentication Guidance

<https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf>

PCI DSS 3.2 Summary of Changes

[https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-2\\_Summary\\_of\\_Changes.pdf?agreement=true&time=1487349929687](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_Summary_of_Changes.pdf?agreement=true&time=1487349929687)

PCI DSS version 3.2 Requirements and Security Assessment Procedures

[https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-2.pdf?agreement=true&time=1487349929647](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1487349929647)

# APPENDIX

For your reference and convenience, we've included Links to HALOCK's Previous guides.

### Guide to PCI DSS 3.1

<https://www.halock.com/-download-pci-3-1-guide-pages-492.php>

### Guide to PCI DSS 3.0

<https://www.halock.com/download-pci-guide-pages-384.php>

**For further guidance to ensure PCI DSS compliance,**  
**[schedule a scoping call with HALOCK](#) to help you through the process.**