“PCI DSS” Dashboard Compliance List

NO:	Dashboard Name	PCI DSS Standard Control Number	Description
1	Compliance- PCI DSS- Host Configuration Change Summary	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 theCDE 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 ofthe computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.
		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.
		2.2.6	System security parameters are configured to prevent misuse.
		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
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		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.
2	Compliance- PCI DSS - Data Transfer Summary	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
		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.
3	Compliance- PCI DSS - User Priv Escalation (Windows) Summary	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.
		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
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities

		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.
4	Compliance- PCI DSS - Software Installed Summary	6.3.2.a	Examine documentation and interview personnel to verify that an inventory of bespoke and custom software and third-party software components incorporated into bespoke and custom software is maintained, and that the inventory is used to identify and address vulnerabilities.
		6.3.2.b	Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.
		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
5	Compliance- PCI DSS - Software Uninstalled Summary	6.3.2.a	Examine documentation and interview personnel to verify that an inventory of bespoke and custom software and third-party software components incorporated into bespoke and custom software is maintained, and that the inventory is used to identify and address vulnerabilities.
		6.3.2.b	Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.
		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).
		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
6	Compliance- PCI DSS - Remote Desktop Protocol Summary	1.2.1	Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained
		1.2.5	All services, protocols, and ports allowed are identified, approved, and have a defined business need
		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

		1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.
		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.
7	Compliance- PCI DSS - Monitoring Linux Processes	2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
		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)
8	Compliance- PCI DSS - Failed File System Access (Windows)	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.
		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.
		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
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		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.
		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.
9	Compliance- PCI DSS - Audit Log Summary	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.

		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)
10	Compliance- PCI DSS - Detailed File Share Summary	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.
		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
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		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.
11	Compliance- PCI DSS - Suspected Wireless Connection Attempt Summary	1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.
		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.
		1.2.2.c	Examine network configuration settings to identify changes made to configurations of NSCs.Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1
12	Compliance- PCI DSS - Critical Environment Error Summary	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.
13	Compliance- PCI DSS - Failure Credential-validated Summary	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.
		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.
		1.2.2.c	Examine network configuration settings to identify changes made to configurations of NSCs.Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1
14		1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties

	Compliance- PCI DSS - Social Media Summary	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.
15	Compliance- PCI DSS - Failed File System Access (Linux)	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.
		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.
		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
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		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.
		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.
16	Compliance- PCI DSS - Rejected Connection to Network	1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.
		1.4.1	NSCs are implemented between trusted and untrusted networks.
		1.4.4	System components that store cardholder data are not directly accessible from untrusted networks
		1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied
		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
17	Compliance- PCI DSS - Detected Virus/Spyware Summary	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

		5.2.2	5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.
		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
		5.3.1	The anti-malware solution(s) is kept current via automatic updates
		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.
		5.2.3.1.a	Examine the entity's targeted risk analysis for the frequency of periodic evaluations of system components identified as not at risk for malware to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1
		5.2.3.1.b	Examine documented results of periodic evaluations of system components identified as not at risk for malware and interview personnel to verify that evaluations are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement
		5.3.2.a	Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution(s) is configured to perform at least one of the elements specified in this requirement.
		5.3.2.b	Examine system components, including all operating system types identified as at risk for malware, to verify the solution(s) is enabled in accordance with at least one of the elements specified in this requirement
		5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1
		10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis
18	Compliance- PCI DSS - System File Permission Change (Linux)	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.
		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.
		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
		7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities
		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.

		1.2.2.c	Examine network configuration settings to identify changes made to configurations of NSCs.Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1
19	Compliance- PCI DSS - Monitoring External Device Access	2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
		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
20	Compliance- PCI DSS - Detecting Brute Force Attack Summary	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
		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.
21	Compliance- PCI-DSS - Physical Security Summary	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.
22	Compliance- PCI-DSS - Unknown User Account Detail	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.
23	Compliance- PCI-DSS - Time Sync Error Summary	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

		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.
24	Compliance- PCI-DSS - System Log File Deletion Summary (Linux)	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.
25	Compliance- PCI-DSS - WebServer Access Logs Deleted Summary	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
		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.
		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.