Telrock Systems
SMARTER TECHNOLOGY, BETTER RESULTS

Telrock Systems PCI DSS Third-Party Service Provider / Merchant Responsibilities Matrix

Telrock Systems SaaS Control Coverage: PCI DSS 4.0.1 Requirement 12.8.5 Compliance

This document has been written for Telrock Systems Clients who wish to utilize Telrock Systems' Cloud SaaS based applications.

PCI DSS v4.0.1 Requirement 12.8.5 states that third-party service providers (TPSPs), merchants and other entities shall: Maintain information about which PCI DSS requirements are managed by each TPSP, and which are managed by the entity.

This document should be utilized by Telrock Systems Clients and their Information Security/Vendor Risk Management department(s), to identify the PCI DSS 4.0.1 scope and control responsibility that both Telrock Systems and the Client shall be held accountable for compliance. It is a breach of PCI DSS compliance to store any payment card security authentication data (SAD) (e.g. security code, PIN, full magnetic stripe data, and dynamic CVV) after transaction authorization, even if SAD is encrypted. Clients are therefore prohibited to use any form of transaction recording which will allow the storage of SAD within the Telrock Systems Cloud hosted application service environment. If applicable for processing, payment card Primary Account Number (PAN) is stored in an encrypted format. Use of Telrock Systems private Cloud services does not relieve the Client of responsibility for its own PCI DSS compliance commitments.

Date	Version	Description of Changes	Owner
11.08.2019	1	1st Draft	Arun Balodi (IT Security Manager)
02.12.2019	2	Top fields changed, change references to company name. Typos fixed	Dale Williams (CEO)
05.12.2019	3	Amended contents in red - change of ownership on certain requirements	Arun Balodi (IT Security Manager)
20.07.2020	4	Created Worksheets per requirements and added PCI Council Guidelines (Reference - https://www.pcisecuritystandards.org/document_library)	Arun Balodi (IT Security Manager)
24.07.2020	4.1	Appendix requirements added	Arun Balodi (IT Security Manager)
30.07.2020	4.2	Document tweaked with more simplified ownership and tasks definition	Arun Balodi (IT Security Manager)
30.06.2021	5	Annual review and ownership change	Ray Jackson (CISO)
15.12.2022	6	Annual review & changes: Coversheet; 3.1; 6.2; 6.4.3; 6.4.4; 6.7; 8.1; 8.2; 8.3; 8.4; 8.5; 8.6; 8.8; 10.1; 10.6; 10.7; 10.9	Ray Jackson (CISO)
03.12.2023	6	Annual review & no changes	Ray Jackson (CISO)
01.10.2024	7	Annual review & changes: Aligned to PCI DSS v4.0 & PCI SSC Information Supplement: Third-Party Assurance (Appendices A & B), coversheet	Ray Jackson (CISO)
03.01.2025	8	Update: Aligned to PCI DSS v4.0.1	Ray Jackson (CISO)

Requirement 1: Install and Maintain Network Security Controls

	Responsibility					
PCI DSS v4.0.1 Requirements	TPSP only	Entity only	Shared	Specific coverage / scope of entity responsibility	Specific coverage / scope of TPSP responsibility	How and when TPSP will provide evidence of compliance to entity
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.	☑	☐	☐		All security policies and operational procedures, that are required to install and maintain network security controls within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
1.2 Network security controls (NSCs) are configured and maintained.	☑	☐	☐		Network security controls within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
1.3 Network access to and from the cardholder data environment is restricted.	☑	☐	☐		Network security controls within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
1.4 Network connections between trusted and untrusted networks are controlled.	☑	☐	☐		Network security controls within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.	☑	☐	☐		Telrock System IT user endpoints that directly connect to Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 2: Apply Secure Configurations to All System Components

	Responsibility					
PCI DSS v4.0.1 Requirements	TPSP only	Entity only	Shared	Specific coverage / scope of entity responsibility	Specific coverage / scope of TPSP responsibility	How and when TPSP will provide evidence of compliance to entity
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.	☑	☐	☐		All security policies and operational procedures, that are required to securely configure all in-scope system components within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
2.2 System components are configured and managed securely.	☑	☐	☐		Secure configuration of in-scope system components within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
2.3 Wireless environments are configured and managed securely.	☑	☐	☐		Not Applicable - No Wireless technologies used within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 3: Protect Stored Account Data

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
3.1 Processes and mechanisms for protecting stored account data are defined and understood.	☐	☐	☑	Data retention and disposal policies, procedures, and processes, required for Client's legal, regulatory, and business requirements. Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood	All security policies and operational procedures, that are required to protect stored payment card account data within Optimus & SmartConnect Application Hosting, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
3.2 Storage of account data is kept to a minimum.	☐	☐	☑	Implementation of data retention and disposal policies, procedures, and processes to ensure storage of account data within the Telrock SaaS solution is kept to a minimum	Provision technology or support a manual process for an entity to securely delete or render account data unrecoverable, when no longer needed per the retention policy. Provision technology or support a manual process for an entity to verify that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable, ensuring that all geographic instances of a data element are securely deleted	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
3.3 Sensitive authentication data (SAD) is not stored after authorization.	☐	☑	☐	Implementation of policies, procedures, processes to ensure sensitive authentication data (SAD) is not stored within the Telrock SaaS solution after authorization, even if encrypted		Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 3: Protect Stored Account Data

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
3.4 Access to displays of full PAN and ability to copy PAN are restricted.	☐	☐	☑	Implementation of policies, procedures, processes and business justifications for masking and allowing the display and of PANs within the Telrock SaaS solution. Provision technology that prevents copy and/or relocation of PAN from within the Telrock SaaS solution	Provision technology to ensure PAN is masked when displayed such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
3.5 Primary account number (PAN) is secured wherever it is stored.	☐	☐	☑	Implementation of policies, procedures, processes to ensure PAN is rendered unreadable anywhere it is stored within the Telrock SaaS solution	Provision technology to provide entities interconnection to a preferred Token Service Provider (TSP), and storage level and / or database encryption mechanisms, to ensure PAN is rendered unreadable anywhere it is stored	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
3.6 Cryptographic keys used to protect stored account data are secured.	☑	☐	☐		Within Optimus & SmartConnect Application Hosting, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.	☑	☐	☐		Within Optimus & SmartConnect Application Hosting, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood.	☐	☐	☑	All security policies and operational procedures, that are required to ensure strong cryptography and security protocols are implemented to safeguard PAN during transmission over open, public networks, are documented. Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood	All security policies and operational procedures, that are required to ensure strong cryptography and security protocols are implemented to safeguard PAN during transmission over open, public networks, are documented. Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
4.2 PAN is protected with strong cryptography during transmission	☐	☐	☑	When transmitting bulk data to / from entity managed host systems, protect PAN with strong cryptography during transmission over open, public networks and maintain an inventory of trusted keys and certificates	Protect PAN with strong cryptography during transmission over open, public networks and maintain an inventory of trusted keys and certificates. No Wireless technologies used within Optimus & SmartConnect Application Hosting, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 5: Protect All Systems and Networks from Malicious Software

	Responsibility					
PCI DSS v4.0.1 Requirements	TPSP only	Entity only	Shared	Specific coverage / scope of entity responsibility	Specific coverage / scope of TPSP responsibility	How and when TPSP will provide evidence of compliance to entity
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.	☐	☐	☑	All security policies and operational procedures, that are required to protect all IT user endpoints that connect to the Optimus Collector Workbench from malicious software, , are documented. Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood	All security policies and operational procedures, that are required to protect all systems and networks from malicious software, within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
5.2 Malicious software (malware) is prevented, or detected and addressed.	☐	☐	☑	Prevent, detect and remediate malware on all Client IT user endpoints that connect to the Optimus Collector Workbench	Prevent, detect and remediate malware on all in-scope system components within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.	☐	☐	☑	Maintain and monitor malware protection mechanisms on all Client IT user endpoints that connect to the Optimus Collector Workbench	Maintain and monitor malware protection mechanisms on all in-scope system components within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
5.4 Anti-phishing mechanisms protect users against phishing attacks.	☐	☐	☑	Implement processes and automated mechanisms to detect and protect Client personnel against phishing attacks against Client IT user endpoints that connect to the Optimus Collector Workbench	Implement processes and automated mechanisms to detect and protect Telrock Systems IT user endpoints that connect to Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 6: Develop and Maintain Secure Systems and Software

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.	☐	☐	☑	All security policies and operational procedures, to verify that processes are defined which prevent the use of live PANs in non-production environments, and removal of test data and test accounts from system components before the system goes into production. Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood	All security policies and operational procedures, that are required to develop and maintain secure systems and software within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
6.2 Bespoke and custom software are developed securely.	☑	☐	☐		Optimus & SmartConnect applications, Telrock Systems development, DevOps and InfoSec teams, and application delivery pipelines	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
6.3 Security vulnerabilities are identified and addressed.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
6.4 Public-facing web applications are protected against attacks.	☑	☐	☐		Optimus & SmartConnect Application Hosting and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
6.5 Changes to all system components are managed securely.	☐	☐	☑	Change authorization, and "post-change" testing and validation support to the Telrock Systems Client Support Team. Assurance that live PANs are not used in pre-production environments and test data and test accounts are removed from system components before the system goes into production	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

	Responsibility					
PCI DSS v4.0.1 Requirements	TPSP only	Entity only	Shared	Specific coverage / scope of entity responsibility	Specific coverage / scope of TPSP responsibility	How and when TPSP will provide evidence of compliance to entity
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	☐	☐	☑	All security policies and operational procedures, that are required to restrict access to Optimus & SmartConnect application and cardholder data, by business need to know, are documented. Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood	All security policies and operational procedures, that are required to restrict access to system components and cardholder data by business need to know, within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
7.2 Access to system components and data is appropriately defined and assigned.	☐	☐	☑	All client staff and consumer Optimus & SmartConnect application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
7.3 Access to system components and data is managed via an access control system(s).	☐	☐	☑	All client staff and consumer Optimus & SmartConnect Application access rights and privilege allocation	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 8: Identify Users and Authenticate Access to System Components

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.	☐	☐	☑	All security policies and operational procedures, that are required to restrict access to Optimus & SmartConnect applications and cardholder data, through appropriate identification and authentication mechanisms, are documented. Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood	All security policies and operational procedures, that are required to restrict access to system components through appropriate identification and authentication mechanisms, within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	☐	☐	☑	All client staff Optimus & SmartConnect application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
8.3 Strong authentication for users and administrators is established and managed.	☐	☐	☑	All client staff Optimus & SmartConnect application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.	☐	☐	☑	All client staff Optimus application access via SFTP	Optimus & SmartConnect Application Hosting and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.	☐	☐	☑	All client staff Optimus & SmartConnect application access, and all client staff Optimus application access via SFTP	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
8.6 Use of application and system accounts and associated authentication factors is strictly managed.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 9: Restrict Physical Access to Cardholder Data

	Responsibility					
PCI DSS v4.0.1 Requirements	TPSP only	Entity only	Shared	Specific coverage / scope of entity responsibility	Specific coverage / scope of TPSP responsibility	How and when TPSP will provide evidence of compliance to entity
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	☑	☐	☐		All security policies and operational procedures, that are required to restrict physical access to system components and cardholder data, within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
9.3 Physical access for personnel and visitors is authorized and managed.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.	☐	☐	☐		Not Applicable - No Point-of-interaction (POI) devices are used within the Optimus or SmartConnect hosted application platforms	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood.	☐	☐	☑	All security policies and operational procedures, that are required to log and monitor all access to the Optimus application, are documented. Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood	All security policies and operational procedures, that are required to log and monitor all access to system components and cardholder data, within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	☐	☐	☑	All client staff Optimus application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
10.3 Audit logs are protected from destruction and unauthorized modifications.	☐	☐	☑	All client staff Optimus application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.	☐	☐	☑	All client staff Optimus application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data (continued)

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
10.5 Audit log history is retained and available for analysis.	☐	☐	☑	All client staff Optimus application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
10.6 Time-synchronization mechanisms support consistent time settings across all systems.	☐	☐	☑	All client staff Optimus application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.	☐	☐	☑	All client staff Optimus application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 11: Test Security of Systems and Networks Regularly

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.	☑	☐	☐		All security policies and operational procedures, that are required to regularly test all system components and networks, within Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
11.5 Network intrusions and unexpected file changes are detected and responded to.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
11.6 Unauthorized changes on payment pages are detected and responded to.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 12: Support Information Security with Organizational Policies and Programs

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.	☐	☐	☑	All security policies and operational procedures, that are required to support Telrock Systems clients Information Security program, including cardholder data protection governance and compliance, risk management, security education and awareness, insider threat screening, supply chain risk management, and information security incident management, scoped against Optimus & SmartConnect applications and cardholder data, are documented. Roles and responsibilities for performing activities in Requirement 12 are documented, assigned, and understood	All security policies and operational procedures, that are required to support Telrock Systems Information Security program, including cardholder data protection governance and compliance, risk management, security education and awareness, insider threat screening, supply chain risk management, and information security incident management, scoped against Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments, are documented. Roles and responsibilities for performing activities in Requirement 12 are documented, assigned, and understood	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
12.2 Acceptable use policies for end-user technologies are defined and implemented.	☐	☐	☑	All client staff Optimus & SmartConnect application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.	☐	☐	☑	All client staff Optimus & SmartConnect application access and processing of cardholder data at client commissioned Token Service Provider (TSP)	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Requirement 12: Support Information Security with Organizational Policies and Programs

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
12.4 PCI DSS compliance is managed.	☐	☐	☑	All client staff Optimus & SmartConnect application access and processing of cardholder data at client commissioned Token Service Provider (TSP)	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
12.5 PCI DSS scope is documented and validated.	☐	☐	☑	All client staff Optimus & SmartConnect application access and processing of cardholder data at client commissioned Token Service Provider (TSP)	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
12.6 Security awareness education is an ongoing activity.	☐	☐	☑	All client staff Optimus & SmartConnect application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
12.7 Personnel are screened to reduce risks from insider threats.	☐	☐	☑	All client staff Optimus & SmartConnect application access	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.	☐	☐	☑	All client staff Optimus & SmartConnect application access and processing of cardholder data at client commissioned Token Service Provider (TSP)	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.	☑	☐	☐		Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	☐	☐	☑	All client staff Optimus & SmartConnect application access and processing of cardholder data at client commissioned Token Service Provider (TSP)	Optimus & SmartConnect Application Hosting, Application Delivery Pipelines, Reporting, and Disaster Recovery IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

	Responsibility					
PCI DSS v4.0.1 Requirements	**TPSP only**	**Entity only**	**Shared**	**Specific coverage / scope of entity responsibility**	**Specific coverage / scope of TPSP responsibility**	**How and when TPSP will provide evidence of compliance to entity**
A1.1 Multi-tenant service providers protect and separate all customer environments and data.	☑	☐	☐		Optimus & SmartConnect Application Hosting IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)
A1.2 Multi-tenant service providers facilitate logging and incident response for all customers.	☑	☐	☐		Optimus & SmartConnect Application Hosting IT environments	Telrock Systems PCI DSS Annual Independent Quality Security Assessor's (QSA) Attestation of Compliance (AOC)