OpenEye®

PCI COMPLIANCE REVIEW

LIBERTY LAKE, WA • 509.232.5261 • WWW.OPENEYE.NET

OpenEye®
PCI Compliance Review
Edition 32604AD – FEBRUARY 2017

OPENEYE
Liberty Lake, WA ● U.S.A.

TABLE OF CONTENTS

PCI COMPLIANCE AND OPENEYE

This document reviews PCI compliance requirements when using OpenEye recorders at a location where cardholder data is processed. It is always important to follow PCI standards to ensure the integrity of networks and sensitive information.

The information contained in this document is provided for reference purposes only and is subject to change at any time. OpenEye provides this information as is and makes no representations that the information is correct or will work for your particular application. OpenEye strongly encourages you to contact your QSA for detailed information about installing OpenEye products in a PCI compliant manner.

OpenEye is not affiliated with the PCI Security Standards Council. The PCI specifications and the information provided below are for convenience purposes only.

WHAT IS PCI?

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. The objective of the PCI standards is to prevent debit or credit card information from being stolen. The two primary concepts of PCI are:

1. Ensure that all hardware/software that process and store cardholder data are separated on the network from the hardware/software that have nothing to do with the cardholder data. This protected area on the network is called the Cardholder Data Environment (CDE).
2. Ensure that processes are in place throughout the organization to protect the CDE.

PCI STANDARDS

The requirements for meeting PCI standards are broken up into 12 key areas:

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

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

DEPLOYMENT

OpenEye has reviewed an OpenEye recorder deployment and how it impacts PCI compliance. This deployment covers the majority of installations, but the concepts discussed here can also apply to other installations.

1. *The OpenEye recorder is installed outside the Cardholder Data Environment*

In this deployment, there is no impact to PCI compliance as long as the OpenEye recorder remains outside the CDE.

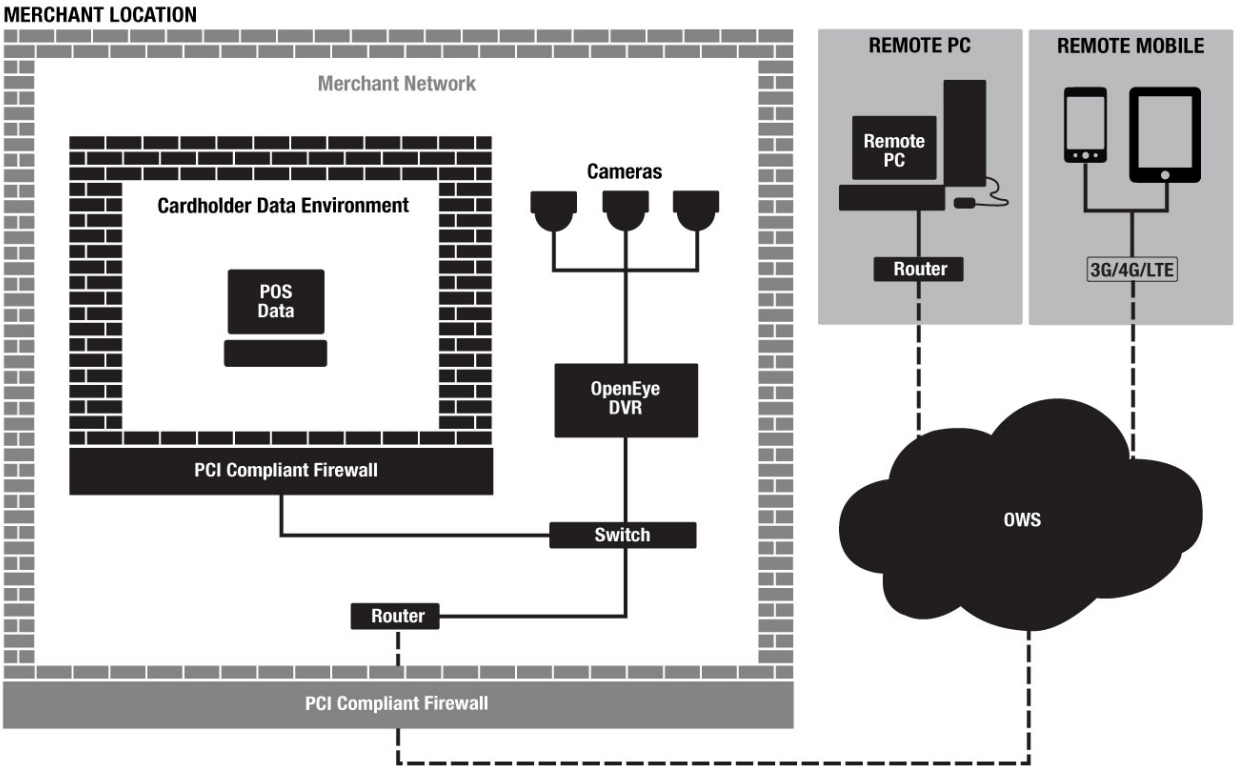
When deploying the OpenEye recorder using the methods discussed in this document, it is our opinion that the OpenEye recorder cannot be used as a gateway or bridge to the cardholder data environment.

DEPLOYMENT 1

The OpenEye recorder is installed outside the Cardholder Data Environment (CDE). In this deployment, there is no impact to PCI compliance as long as the OpenEye recorder remains outside the CDE.

Figure 1

Deployment scenario 1 / OpenEye recorder outside of CDE



Deployment

- The OpenEye recorder must be isolated from the CDE to ensure that PCI compliance is not impacted.
- It is important to pay careful attention to how cameras are positioned. They should not be positioned in such a way that cardholder information can be seen and recorded.
- Always change default passwords for the recorder and cameras.
- Use strong passwords consisting of both letters and numbers that are at least 7 characters long.

  Tip - The strongest passwords should also contain both upper and lowercase letters along with special characters (!@#$%).
- Create unique user accounts for each user who accesses the recorder. Do not use the default built-in Admin account.
- Restrict administrator permissions on the recorder to only those who need it.
- Enable 2-step authentication for all OWS user accounts.
- Install OpenEye security patches within one month of release.

- When recording sensitive areas of the CDE, store video for three months. See section 9.1.1.
- When using the OpenEye Remote software on the merchant network, the PC must be properly segmented from the CDE using a properly configured firewall meeting PCI requirements for segmentation.
- Even though the OpenEye recorder will reside on the merchant network but remain outside the CDE, the merchant standard network policies pertaining to PC devices should be enforced.

PCI DDS COMPLIANCE

The following table outlines each of the PCI DDS 3.2 requirements and provides an overview of how each of the deployments impacts the requirements. This chart is just an overview, and each of the items should be reviewed more in-depth by your PCI compliance officer.

Legend

 Has no impact on PCI compliance

 Has an impact on PCI compliance

REQUIREMENT 1

Install and maintain a firewall configuration to protect cardholder data.

PCI DSS Requirements	Recorder is outside CDE	Notes
1.1 Establish and implement firewall and router configuration standards that include the following:		*All Firewall configurations and rules must be documented and adhered to.* Note: Since Firewalls provide protection against attacks, the merchant must ensure that that it has strong firewall configuration standards. The OpenEye recorder must be isolated from the Cardholder Data Environment (CDE).The OpenEye recorder does not operate in place of devices required for perimeter security.
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations		See 1.1
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks		See 1.1
1.1.3 Current diagram that shows all cardholder data flows across systems and networks		See 1.1

PCI DSS Requirements	Recorder is outside CDE	Notes
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone		See 1.1
1.1.5 Description of groups, roles, and responsibilities for management of network components		See 1.1
1.1.6 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.		See 1.1
1.1.7 Requirement to review firewall and router rule sets at least every six months		
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.		See 1.1 *Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.		See 1.1
1.2.2 Secure and synchronize router configuration files.		See 1.1
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.		*Ensure that all wireless networks are segmented to prevent wireless attackers from gaining access to the CDE and/or other network resources.*
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment**.**		*There should be no direct access into or out of any component in the CDE, including the OpenEye recorder.*
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.		See 1.3
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.		See 1.3

PCI DSS Requirements	Recorder is outside CDE	Notes
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)		See 1.3
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.		See 1.3
1.3.5 Permit only "established" connections into the network.		See 1.3
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.		See 1.3
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.		See 1.3 *Note: Methods to obscure IP addressing may include, but are not limited to:* • Network Address Translation (NAT) • Placing servers containing cardholder data behind proxy servers/firewalls or content caches, • Removal or filtering of route advertisements for private networks that employ registered addressing, • Internal use of RFC1918 address space instead of registered addresses.
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations		*There should be no direct access into or out of any component in the CDE, including the OpenEye recorder.* Note: Only specific IT Administration should have

PCI DSS Requirements	Recorder is outside CDE	Notes
include: • Specific configuration settings are defined. • Personal firewall software (or equivalent functionality) is actively running. • Personal firewall software (or equivalent functionality) is not alterable by users of portable computing devices.		access to critical components in the CDE, and their mobile devices should have personal firewalls installed.
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.		

REQUIREMENT 2

Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirements	Recorder is outside CDE	Notes
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. 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, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).		Please change the default password for the OpenEye recorder at this point.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.		See 1.2.3
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).		See 2.1 Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)		See 2.1 *Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.*

PCI DSS Requirements	Recorder is outside CDE	Notes
2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system.		See 2.1
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure		See 2.1
2.2.4 Configure system security parameters to prevent misuse.		See 2.1
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.		See 2.1
2.3 Encrypt all non-console administrative access using strong cryptography.		*Prohibit the PC that is running the OpenEye remote software network access to the CDE.* ***Note**: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016.Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.*
2.4 Maintain an inventory of system components that are in scope for PCI DSS.		N/A
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.		

PCI DSS Requirements	Recorder is outside CDE	Notes
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.*		

REQUIREMENT 3

Protect stored cardholder data.

PCI DSS Requirements	Recorder is outside CDE	Notes
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.		*The OpenEye recorder does not collect, store or transmit sensitive cardholder data.* Note - Surveillance cameras should be positioned in such a way that they do not capture cardholder data from the POS or any other sensitive information such as password entry.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:		See 3.1 *Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.*
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.		See 3.1 *Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • The cardholder's name • Primary account number (PAN) • Expiration date • Service code *To minimize risk, store only these data elements as needed for business.*
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.		See 3.1

PCI DSS Requirements	Recorder is outside CDE	Notes
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.		See 3.1
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.		Notes: *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures.		See 3.1 *Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.		See 3.1
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:		See 3.1 *Note: This requirement also applies to key-encrypting keys used to protect data- encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key*.

PCI DSS Requirements	Recorder is outside CDE	Notes
3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management.		See 3.1
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.		
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method		See 3.1 Note: *It is not required that public keys be stored in one of these forms.*
3.5.4 Store cryptographic keys in the fewest possible locations.		
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:		See 3.1 *Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*
3.6.1 Generation of strong cryptographic keys.		See 3.1
3.6.2 Secure cryptographic key distribution.		See 3.1

PCI DSS Requirements	Recorder is outside CDE	Notes
3.6.3 Secure cryptographic key storage.		See 3.1
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher- text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).		See 3.1
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised.		See 3.1 *Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.		See 3.1 *Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*
3.6.7 Prevention of unauthorized substitution of cryptographic keys.		See 3.1
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.		See 3.1
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.		See 3.1

REQUIREMENT 4

Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirements	Recorder is outside CDE	Notes
4.1 Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.		*The OpenEye recorder does not collect, store or transmit sensitive cardholder data. The data transmitted by the recorder is video surveillance. Therefore, there is no need for encryption when sending data between the OpenEye recorder and the remote clients.*
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.		See 1.2.3 and 4.1 *Note: The use of WEP as a security control was prohibited as of 30 June 2010.*
4.2 Never send unprotected PANs by end-user messaging technologies (for example, email, instant messaging, chat, etc.).		See 4.1
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.		See 4.1

REQUIREMENT 5

Protect all systems against malware and regularly update antivirus software or programs

PCI DSS Requirements	Recorder is outside CDE	Notes
5.1 Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).		Prohibit the PC that is running OpenEye remote software network access to the CDE. The merchant should install an up–to-date antivirus program on the OpenEye recorder. Please refer to FAQ 154 on http://www.openeye.net for further information on installing antivirus on the OpenEye recorder.
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.		See 5.1 *Note: Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.*
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.		See 5.1
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.		See 5.1
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.		***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*

PCI DSS Requirements	Recorder is outside CDE	Notes
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.		

REQUIREMENT 6

Develop and maintain secure systems and applications

PCI DSS Requirements	Recorder is outside CDE	Notes
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.		All software updates for the OpenEye recorder should be installed in a timely manner to help reduce the risk of penetration and vulnerability based attacks and exploits. *Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.		See 6.1 *Notes: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging)		*Note: This applies to all software developed internally as well as bespoke or custom software developed by a third party.*

PCI DSS Requirements	Recorder is outside CDE	Notes
• Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle		
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.		See 6.3
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.		See 6.3 *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.* *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:		*Any changes to components or systems within the CDE should be documented according to the change control requirements.*
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.		See 6.4
6.4.2 Separation of duties between development/test and production environments.		See 6.4
6.4.3 Production data (live PANs) are not used for testing or development.		See 6.4
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.		See 6.4

PCI DSS Requirements	Recorder is outside CDE	Notes
6.4.5 Change control procedures must include the following:		See 6.4
6.4.5.1 Documentation of impact.		See 6.4
6.4.5.2 Documented change approval by authorized parties.		See 6.4
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.		See 6.4
6.4.5.4 Back-out procedures.		See 6.4
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.		See 6.4
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines.		See 6.3 *Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.		See 6.3
6.5.2 Buffer overflows		See 6.3
6.5.3 Insecure cryptographic storage		See 6.3
6.5.4 Insecure communications		See 6.3
6.5.5 Improper error handling		See 6.3

PCI DSS Requirements	Recorder is outside CDE	Notes
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).		See 6.3
6.5.7 Cross-site scripting (XSS)		See 6.3
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).		See 6.3
6.5.9 Cross-site request forgery (CSRF)		See 6.3
6.5.10 Broken authentication and session management		See 6.3
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.		See 6.3
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.		See 6.3

REQUIREMENT 7

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

PCI DSS Requirements	Recorder is outside CDE	Notes
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.		Only specific IT Administrators should have access to critical components in the CDE. Merchants should manage access to the OpenEye recorder when it resides within the CDE.
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.		See 7.1
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.		See 7.1
7.1.3 Assign access based on individual personnel's job classification and function.		See 7.1
7.1.4 Require documented approval by authorized parties specifying required privileges.		N/A – The OpenEye recorder has authentication-based access enabled by default.
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:		See 7.1
7.2.1 Coverage of all system components		See 7.1
7.2.2 Assignment of privileges to individuals based on job classification and function		See 7.1
7.2.3 Default "deny-all" setting		See 7.1 *Note: Some access control systems are set by default to allow-all, thereby permitting access unless/until a rule is written to specifically deny it.*
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use,		

PCI DSS Requirements	Recorder is outside CDE	Notes
and known to all affected parties.		

REQUIREMENT 8

Identify and authenticate access to system components

PCI DSS Requirements	Recorder is outside CDE	Notes
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:		*Prohibit the OpenEye recorder and the PC that is running the OpenEye remote software direct access to the CDE. Only specific IT Administrators should have access to critical components in the CDE.*
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.		See 8.1
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.		See 8.1
8.1.3 Immediately revoke access for any terminated users.		See 8.1
8.1.4 Remove/disable inactive user accounts within 90 days.		See 8.1
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.		See 8.1
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.		See 8.1
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.		See 8.1

PCI DSS Requirements	Recorder is outside CDE	Notes
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.		See 8.1
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.		*See 8.1, The OpenEye recorder requires a username and password for access.*
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.		See 8.1
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.		See 8.1
8.2.3 Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.		See 8.1
8.2.4 Change user passwords/passphrases at least once every 90 days.		See 8.1
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.		See 8.1

PCI DSS Requirements	Recorder is outside CDE	Notes
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.		See 8.1
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.		See 8.1
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.		See 8.1 *This requirement is intended to apply to all personnel with administrative access to the CDE. This requirement applies only to personnel with administrative access and only for non-console access to the CDE; it does not apply to application* *or system accounts performing automated functions.* *If the entity does not use segmentation to separate the CDE from the rest of their network, an administrator could use multi-factor authentication either when logging onto the CDE network or when logging onto a system.* *If the CDE is segmented from the rest of the entity's network, an administrator would need to use multi- factor authentication when connecting to a CDE system from a non-CDE network. Multi-factor authentication can be implemented at network level or at system/application level; it does not have to be both. If the administrator uses MFA when logging into the CDE network, they do not also need to use MFA to log into a particular system or application within the CDE.*
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and		*This requirement is intended to apply to all personnel—including general users, administrators, and*

PCI DSS Requirements	Recorder is outside CDE	Notes
including third-party access for support or maintenance) originating from outside the entity's network.		*vendors (for support or maintenance) with remote access to the network—where that remote access could lead to access to the CDE. If remote access is to an entity's network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data environment, multi-factor authentication for remote access to that network would not be required. However, multi- factor authentication is required for any remote access to networks with access to the cardholder data environment, and is recommended for all remote access to the entity's networks.*
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.		See 8.1 *The OpenEye recorder transmits and securely stores all user passwords. All user passwords on the OpenEye recorder are encrypted.*
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.		*Ensure all OpenEye users have unique user accounts. The admin account should not be used.*

PCI DSS Requirements	Recorder is outside CDE	Notes
8.5.1 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.		See 8.5 **Note:** *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.		See 8.1
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).		See 8.1
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.		See 8.1

REQUIREMENT 9

Restrict physical access to cardholder data

PCI DSS Requirements	Recorder is outside CDE	Notes
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.		*Merchants should have appropriate controls to ensure that the POS terminals cannot be physically altered, that perimeter devices are properly protected, and that any paper receipts (POS receipts being sent to a printer) are protected if they contain primary account numbers.*
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.		See 9.1 *When investigating physical breaches, these controls can help identify the individuals that physically accessed the sensitive areas, as well as when they entered and exited.* *Criminals attempting to gain physical access to sensitive areas will often attempt to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, access control mechanisms could be monitored or have physical protections installed to prevent them being damaged or disabled by malicious individuals.*
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks.		See 9.1 *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.*

PCI DSS Requirements	Recorder is outside CDE	Notes
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.		See 9.1
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).		See 9.1 *Merchants should ensure that there is basic training to ensure that unauthorized visitors cannot access POS terminals or Camera placements.*
9.3 Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.		See 9.2
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:		See 9.2
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.		See 9.2
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.		See 9.2
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.		See 9.2
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three		See 9.2

PCI DSS Requirements	Recorder is outside CDE	Notes
months, unless otherwise restricted by law.		
9.5 Physically secure all media.		*The OpenEye recorder does not collect, store or transmit sensitive cardholder data. Therefore there is no impact to this requirement or need for offsite storage.*
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.		See 9.5
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:		*Merchants should have appropriate controls to ensure that any paper receipts (POS receipts being sent to a printer) are protected if they contain cardholder data. It is the responsibility of the merchant to ensure that the POS is printing the PAN in a PCI DSS / PA DSS compliant manner and that full PAN is not printed.*
9.6.1 Classify media so the sensitivity of the data can be determined.		See 9.6
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.		See 9.6
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).		See 9.6
9.7 Maintain strict control over the storage and accessibility of media.		See 9.6
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.		See 9.6
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:		See 9.6
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.		See 9.6
9.8.2 Render cardholder data on electronic media unrecoverable so that		See 9.6

PCI DSS Requirements	Recorder is outside CDE	Notes
cardholder data cannot be reconstructed.		
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.		See 9.6
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.		See 9.6
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).		***Note:*** *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).		
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all		

PCI DSS Requirements	Recorder is outside CDE	Notes
affected parties.		

REQUIREMENT 10

Track and monitor all access to network resources and cardholder data

PCI DSS Requirements	Recorder is outside CDE	Notes
10.1 Implement audit trails to link all access to system components to each individual user.		*Security best practices include the use of logging and establishing secure audit trails to identify who did what, and when. Since the OpenEye recorder is not installed in the CDE, this requirement is not applicable.*
10.2 Implement automated audit trails for all system components to reconstruct the following events:		See 10.1
10.2.1 All individual accesses to cardholder data		See 10.1
10.2.2 All actions taken by any individual with root or administrative privileges		See 10.1
10.2.3 Access to all audit trails		See 10.1
10.2.4 Invalid logical access attempts		See 10.1
10.2 5 Use of identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges		See 10.1
10.2.6 Initialization, stopping, or pausing of the audit logs		See 10.1
10.2.7 Creation and deletion of system-level objects		See 10.1
10.3 Record at least the following audit trail entries for all system components for each event:		See 10.1
10.3.1 User identification		See 10.1
10.3.2 Type of event		See 10.1

PCI DSS Requirements	Recorder is outside CDE	Notes
10.3.3 Date and time		See 10.1
10.3.4 Success or failure indication		See 10.1
10.3.5 Origination of event		See 10.1
10.3.6 Identity or name of affected data, system component, or resource.		See 10.1
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.		See 10.1 *Note: One example of time synchronization technology is Network Time Protocol (NTP).*
10.4.1 Critical systems have the correct and consistent time.		See 10.1
10.4.2 Time data is protected.		See 10.1
10.4.3 Time settings are received from industry-accepted time sources.		See 10.1
10.5 Secure audit trails so they cannot be altered.		See 10.1
10.5.1 Limit viewing of audit trails to those with a job-related need.		See 10.1
10.5.2 Protect audit trail files from unauthorized modifications.		See 10.1
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.		See 10.1
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.		See 10.1
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).		See 10.1

PCI DSS Requirements	Recorder is outside CDE	Notes
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.		See 10.1 *Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).		See 10.1
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.		See 10.1
10.6.3 Follow up exceptions and anomalies identified during the review process.		See 10.1
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).		See 10.1
10.8 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are		*This requirement must be performed regardless of the OpenEye recorder installation if a merchant processes, stores, and/or transmits cardholder data.*

PCI DSS Requirements	Recorder is outside CDE	Notes
required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls		
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.		See 10.8

REQUIREMENT 11

Regularly test security systems and processes.

PCI DSS Requirements	Recorder is outside CDE	Notes
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.		*This requirement must be performed regardless of the OpenEye recorder installation if a merchant processes, stores, and/or transmits cardholder data.* *Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.		See 11.1
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.		See 11.1
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).		*This requirement must be performed regardless of the OpenEye recorder installation if a merchant processes, stores, and/or transmits cardholder data.* *Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity* *has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re- scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.*
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement		*This requirement must be performed regardless of the OpenEye recorder installation if a merchant processes, stores, and/or transmits cardholder data.*

PCI DSS Requirements	Recorder is outside CDE	Notes
6.1). Scans must be performed by qualified personnel.		
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.		See 11.2 *Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.*
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.		See 11.2 *Note: Scans conducted after changes may be performed by internal staff.*
11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.		*This requirement must be performed regardless of the OpenEye recorder installation if a merchant processes, stores, and/or transmits cardholder data.*

PCI DSS Requirements	Recorder is outside CDE	Notes
11.3.1 Perform *external* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		See 11.3
11.3.2 Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		See 11.3
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.		See 11.3
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.		See 11.3
11.3.4.1 Additional requirement for service providers only: 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.		See 11.3
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.		See 11.3
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and		*This requirement must be performed regardless of the OpenEye recorder installation if a merchant processes, stores, and/or transmits cardholder data.* *Note: For change-detection*

PCI DSS Requirements	Recorder is outside CDE	Notes
configure the software to perform critical file comparisons at least weekly.		*purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.		See 11.5
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.		See 11.3

REQUIREMENT 12

Maintain a policy that addresses information security for all personnel.

PCI DSS Requirements	DVR is outside CDE	Notes
12.1 Establish, publish, maintain, and disseminate a security policy.		*This requirement must be performed regardless of the OpenEye recorder installation if a merchant processes, stores, and/or transmits cardholder data.*
12.1.1 Review the security policy at least annually and update the policy when the environment changes.		See 12.1
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and		See 12.1 Note: *Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*

PCI DSS Requirements	DVR is outside CDE	Notes
• Results in a formal, documented analysis of risk.		
12.3 Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following:		See 12.1
12.3.1 Explicit approval by authorized parties		See 12.1
12.3.2 Authentication for use of the technology		See 12.1
12.3.3 A list of all such devices and personnel with access		See 12.1
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)		See 12.1
12.3.5 Acceptable uses of the technology		See 12.1
12.3.6 Acceptable network locations for the technologies		See 12.1
12.3.7 List of company-approved products		See 12.1
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity		See 12.1
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use		See 12.1
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.		See 12.1

PCI DSS Requirements	DVR is outside CDE	Notes
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.		See 12.1
12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication		See 12.1
12.5 Assign to an individual or team the following information security management responsibilities:		See 12.1
12.5.1 Establish, document, and distribute security policies and procedures.		See 12.1
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.		See 12.1
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.		See 12.1
12.5.4 Administer user accounts, including additions, deletions, and modifications		See 12.1
12.5.5 Monitor and control all access to data.		See 12.1
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.		See 12.1
12.6.1 Educate personnel upon hire and at least annually.		See 12.1 *Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.		See 12.1

PCI DSS Requirements	DVR is outside CDE	Notes
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)		See 12.1 *Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:		See 12.1
12.8.1 Maintain a list of service providers including a description of the service provided.		See 12.1
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.		See 12.1 *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.		See 12.1
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.		See 12.1
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.		See 12.1
12.9 ***Additional requirement for service providers only:*** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.		***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*

PCI DSS Requirements	DVR is outside CDE	Notes
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.		See 12.1
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data back-up processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands		See 12.1
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.		See 12.1
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.		See 12.1
12.10.4 Provide appropriate training to staff with security breach response responsibilities.		See 12.1
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.		See 12.1
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.		See 12.1
12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews		See 12.1

PCI DSS Requirements	DVR is outside CDE	Notes
• Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes		
12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program		See 12.1

ADDITIONAL PCI INFORMATION

Website
www.pcisecuritystandards.org

PCI DSS Standards
https://www.pcisecuritystandards.org/security_standards/documents.php

Approved QSA
https://www.pcisecuritystandards.org/approved_companies_providers/index.php

www.openeye.net
1-888-542-1103