EXATE

PCI DSS V4.0 AND DATA PRIVACY

SEPTEMBER 2023 // PREPARED BY ALICE WILD & DANIEL SAUNDERS

INTRODUCTION

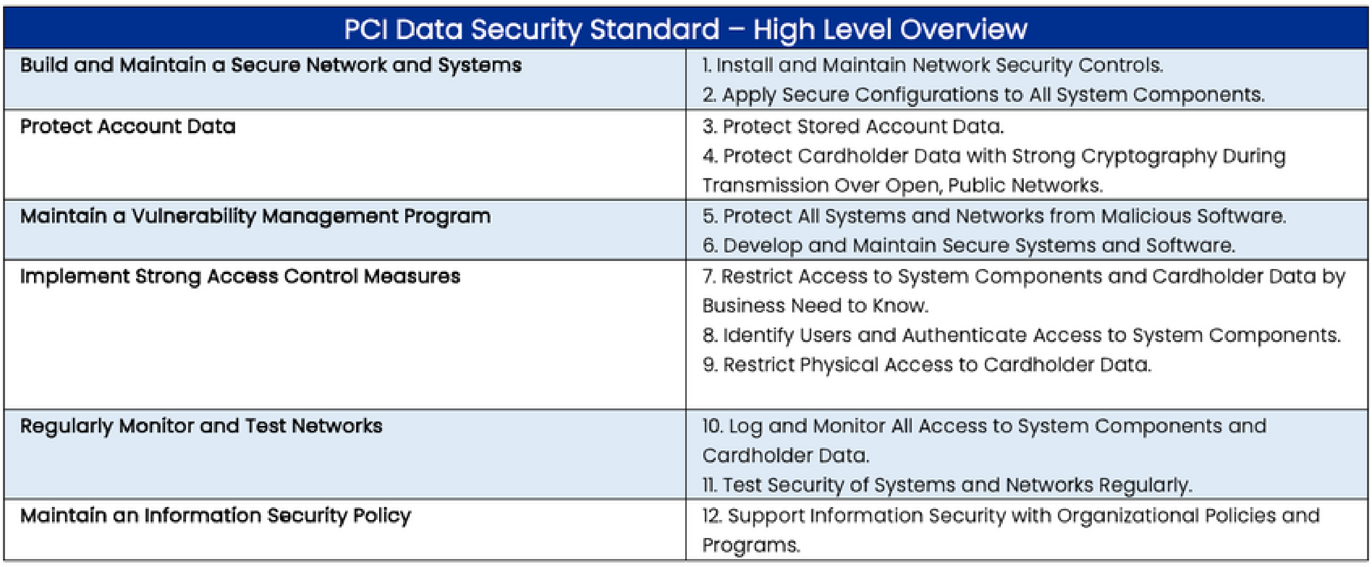
SEPTEMBER 2023

WHAT IS PCI DSS V4.0?

PCI Data Security Standard (PCI DSS) is a global standard that provides a baseline of technical and operational requirements designed to protect account data. Any entity that transmits, stores, handles, or accepts credit card data must adhere to PCI DSS.

PCI DSS 4.0 goes into effect on March 31, 2024. As **APIs play an increasingly significant role in online payments**, the introduction of PCI DSS 4.0 brought with it more stringent security regulations with far-reaching ramifications for data privacy.

PRINCIPLE PCI DSS 4.0 REQUIREMENTS?



PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls. 2. Apply Secure Configurations to All System Components.
Protect Account Data	3. Protect Stored Account Data. 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software. 6. Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know. 8. Identify Users and Authenticate Access to System Components. 9. Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data. 11. Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.

WHICH REQUIREMENTS THAT EXATE WILL COVER?

1. Protect Account Data
    a. Protect Stored Account Data
    b. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
2. Implements Strong Access Control Measures
    a. Restrict Access to System Components and Cardholder Data by Business Need to Know
3. Regularly Monitor and Test Networks
    a. Log and Monitor All Access to System Components and Cardholder Data
        i. Audit logs are protected from destruction and unauthorised modifications
            1. Read access to audit logs files is limited to those with a job-related need.
4. Maintain an information security policy
    a. Support Information Security with Organisational Policies and Programs
        i. Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

PCI DSS 4.0 REQUIREMENTS

PROTECT ACCOUNT DATA

PCI DSS REQUIREMENT: PROTECT ACCOUNT DATA

PROTECT STORED CARDHOLDER DATA

You must know all the data you are going to store along with its location and retention period. All such cardholder data must be protected using one or more industry-accepted techniques such as encrypted, truncation, tokenisation or hashing. The goal is to make any stolen cardholder data unusable.

Where encryption is used, a strong key management process is a must. The scope of PCI DSS covers managing encryption keys and provides detailed guidance on the subject.

ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS

You must know all the data you are going to store along with its location and retention period. All such cardholder data must be protected using one or more industry-accepted techniques such as encrypted, truncation, tokenization or hashing. The goal is to make any stolen cardholder data unusable.

Where encryption is used, a strong key management process is a must. The scope of PCI DSS covers managing encryption keys and provides detailed guidance on the subject.

PCI DSS REQUIREMENT: IMPLEMENTS STRONG ACCESS CONTROL MEASURES

RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW

Service providers and merchants must be able to control access to cardholder data. Cardholder data should be limited to business users and systems on a ‘need to know’ basis, following principles of least privilege.

Role-based access control (RBAC) systems governing access to cardholder data should be based on industry standard authentication and authorization protocols. Access policies should be reviewed regularly to ensure they reflect organisational changes, for example employee cessation, secondment, etc.

Traditionally, firms used RBAC, but It is becoming more and more expensive to use RBAC when attempting to enforce data privacy in the increasingly regulated world around us. Attribute Based Access Control (“ABAC”) draws on a set of characteristics called “attributes.” These can include user attributes, environmental attributes, resource attributes, context attributes, device attributes or even weather attributes. The key differentiator between approaches is that RBAC offers coarse grained control, while ABAC takes a fine-grain approach, possibly using attributes in policies that are not traditional organisational concepts

ACCESS CONTROL MEASURES

MONITOR AND TEST NETWORKS

PCI DSS REQUIREMENT: REGULARLY MONITOR AND TEST NETWORKS

LOG AND MONITOR ALL ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA

All access to cardholder data must be logged, including both successful and unsuccessful attempts. In addition any changes to logging behaviour and access privileges must also be logged.

The log record should be centralised, with access limited to authorised users. The log record should be immutable and monitored on a daily basis, alerts may assist with raising attention to any unusual or suspicious activity.

Audit log files contain sensitive information, and read access to the log files must be limited only to those with a valid business need. This access includes audit log files on the originating systems as well as anywhere else they are stored.

Adequate protection of the audit logs includes strong access control that limits access to logs based on "need to know" only and the use of physical or network segregation to make the logs harder to find and modify

PCI DSS REQUIREMENT: MAINTAIN AN INFORMATION SECURITY POLICY

SUPPORT INFORMATION SECURITY WITH ORGANISATIONAL POLICIES AND PROGRAMS

This is the final requirement of PCI compliance and it is dedicated to the core PCI DSS goal of implementing and maintaining an information security policy for all employees and other relevant parties.

RISK TO INFORMATION ASSETS ASSOCIATED WITH THIRD-PARTY SERVICE PROVIDER (TPSP) RELATIONSHIPS IS MANAGED.

There are new requirements for Third Party Service Providers (“TPSPs), including some new ones only for “multi-tenant service providers”:

- Multi-tenant service providers will be required to confirm that access to the customer environment is logically separated to prevent unauthorised access–and the provider must confirm the effectiveness of those controls.
- Multi-tenant service providers must also implement “processes or mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities”.
- All TPSPs will need to have a documented description of their cryptographic architecture that includes prevention of the use of the cryptographic keys in both the test and production environments.

INFORMATION SECURITY POLICY

EXATE YOUR DATA

WHERE DOES EXATE COME IN?

Here at eXate we can help you tackle these new requirements in respect to data privacy.

eXate is a distributed software platform for enforcing data privacy, data protection, and dynamic Attribute Based Access Control (ABAC) by embedding centralised controls in common data ingestion and distribution points.

EXATE'S KEY FEATURES AND HOW THEY RELATE TO PCI4 REQUIREMENTS

- Data Access Management

"Service providers and merchants must be able to control access to cardholder data."

Using eXate you can quickly and easily revoke or allow access to datasets or individual dataset attributes using the relevant techniques, for the right consumer, in the right form. eXate has been designed to fit as a part of an existing ecosystem, where proprietary data access controls can remain in parallel, and in addition to, new ABAC rules.

WHERE DOES EXATE COME IN?

- Discovery and Remediation

"All such cardholder data must be protected using one or more industry-accepted techniques such as encrypted, truncation, tokenisation or hashing."

To enable the fastest possible ways to protect our data it's unrealistic to expect individuals to know the risks associated with each data attribute and the context it is being used. The eXate platform can analyse a data estate and based upon our analysis and industry models advise of any privacy or security issues or risks that may exist and automatically remediate if necessary.

eXate is an aggregator of Privacy Enhancing Techniques to ensure that data is protected in the right manner, for the right person, in the right job function, in the right location.

- Policy Management

"Implementing and maintaining an information security policy for all employees and other relevant parties."

All policies relating to data sharing can be captured in eXate. This includes policies from departments such as the Data Protection Officer (DPO), Compliance, Legal, the Chief Information Security Officer (CISO), and others, for internal data sharing, external data sharing, and cross border data sharing. As opposed to storing these policies in a Word document or PDF on the Intranet, and leaving the wording open to interpretation, the policies are automatically and consistently applied in the eXate platform.

SECURITY BY DEFAULT

WHERE DOES EXATE COME IN?

- Audit and Reporting

"All access to cardholder data must be logged, including both successful and unsuccessful attempts."

The data flowing through the eXate platform is audited on a granular attribute by attribute basis. Items audited include who tried to access the data, for what purpose, was access granted, if not, then why, and what rules were in place at any time historically.

Additionally, eXate can protect log files with emergency break glass access to specified people.

CONCLUSION

PCI DSS 4 is coming into play on March 31, 2024 with a stronger focus on APIs, data privacy, and data security. These new requirements will be challenging, but there is a solution and we can assist you on your journey to compliance with the privacy aspects

For more information contact info@exate.com or visit our website at www.exate.com