We record & analyze communications

Payment Card Industry Data Security Standard (PCI DSS)

Established by five major credit card schemes – Visa, MasterCard, American Express, Discover, and JCB, the Payment Card Industry Data Security Standard is a security standard for payment card transactions, safeguarding transactions from data theft and fraud.
To comply with the standard, businesses that handle card payment transactions must strictly control access to the personal and financial information of the cardholder, as well as monitoring unauthorized access to the corporate network.

Mitigate Risks with
ASC Technologies' Recording and AI Solutions

Learn more by watching **this short video**.

Payment Card Industry – Data Security Standard

Main Purpose

Governed by the Payment Card Industry Security Standards Council (PCI SSC), the compliance scheme aims to secure credit and debit card transactions against data theft and fraud.

Who Must Comply

All companies that handle or manage credit card data, regardless of their role or industry, must comply with PCI DSS requirements.

PCI DSS Version 4.0

PCI DSS 4.0 is designed to further secure cardholder data by helping organizations take a more holistic view of security measures and access controls. In addition, to respond to new threats posed by advances in technology.

Update Goals

Continue to Meet the Security Needs of the Payment Industry

- Expanded multi-factor authentication requirements.
- Updated password requirements.
- New e-commerce and phishing requirements to address ongoing threats.

Promote Security as Continuous Process

- Clearly assigned roles and responsibilities for each requirement.
- Added guidance to help people better understand how to implement and maintain security.

Add Flexibility for Different Methodologies

- Allowance of group, shared, and generic accounts.
- Targeted risk analyses empower organizations to establish frequencies for performing certain activities.
- Customized approach, a new method to implement and validate PCI DSS requirements, provides another option for organizations using innovative methods to achieve security objectives.

Enhance Validation Methods

- Increased alignment between information reported in a Report on Compliance or Self-Assessment.
- Questionnaire and information summarized in an Attestation of Compliance.

PCI DSS COMPLIANT

Benefits of Compliance

- **Enhanced Security:** PCI DSS compliance helps businesses establish and maintain robust security measures to protect sensitive payment card information. By adhering to the standard's requirements, organizations can reduce the risk of data breaches, fraud, and unauthorized access.

- **Customer Trust and Confidence:** Demonstrating compliance with PCI DSS can enhance customer trust and confidence in your organization. Customers are more likely to trust businesses that prioritize the security of their payment card data, leading to increased customer satisfaction and loyalty.

- **Legal and Regulatory Compliance:** Compliance with PCI DSS helps businesses meet legal and regulatory requirements related to the protection of payment card data. Failure to comply with PCI DSS may result in fines, penalties, and legal liabilities, so adherence to the standard is essential for mitigating these risks.

How can ASC Help with Compliance?

Aside from compliance regulations set by organizations like PCI DSS and rules under MiFID II, Dodd-Frank, and FINRA companies also need to comply with data security regulations like the GDPR. ASC's solutions makes sure that companies meet both regulatory requirements. Designed for today's modern communications environments ASC make it secure and easy to comply with the highest data security standards and sets its solutions apart from others.

- AI helps instantly detect potential compliance breaches
- Configurable recording rules, access rights
- Secure and selectable storage & archiving options
- Tenant-specific data encryption / bring your own key
- Approval process for access and replay
- Customizable retention times & secure deletion process
- Audit-log reports