DATA SECURITY 101

What is PCI Compliance and why is it important?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of technical and operational standards developed to encourage and enhance payment card data security. Applicable to all merchants, regardless of size, PCI compliance helps protect you and your customers from data compromise.

Implementing PCI DSS helps to minimize the risk of a data security incident while you maximize customer trust.

The PCI Data Security Standard

Adopted by the Payment Brands and applicable to all entities that process, store or transmit cardholder data and/or sensitive authentication data, the goal of PCI DSS is to promote safe payments worldwide.

Goals	PCI DSS Requirements
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

What are the American Express Data Security Requirements?

- Comply with the current PCI Data Security Standards
- Store cardholder data only as needed to facilitate American Express Card transactions
- Use only PCI-approved PIN Entry Devices or Payment Applications
- Provide PCI DSS validation documentation to American Express, as required
- Notify American Express when you experience a data security incident within 72 hours of discovery
- Adhere to applicable indemnity obligations resulting from a Data Security Incident

What to do if you have a data incident?

Step 1

Immediately send an email to EIRP@aexp.com no later than 72 hours after the incident is discovered.

Step 2

Conduct a thorough investigation that may require you to hire a Payment Card Industry (PCI) Forensic Investigator.

Step 3

Promptly provide us with all compromised American Express® Card numbers.

Step 4

Work with us to help resolve any issues arising from the data incident.

Learn more about the American Express Data Security Operating Policy at **americanexpress.com/datasecurity**.