PCI101 - PCI-DSS Compliance

Course Learning Objectives

Define the terminology specific to PCI-DSS, describe the entities that must comply with PCI-DSS, and state the 12 requirements of PCI-DSS.
How to protect data and prevent vulnerabilities from becoming a problem for you.
How to protect cardholder data in storage and in transit, enforce strong access control measures, and create an information security policy for your organization.
Describe the guidelines and best practices for building and maintaining secure networks and systems.
Develop a program that identifies and manages vulnerabilities using industry standards.

Description

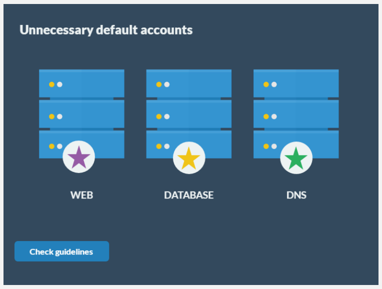
This course is designed to provide PCI-DSS awareness training to individuals with PCI-DSS compliance responsibilities. In this course, you will gain fundamental knowledge of PCI to develop effective security responsibilities, safeguards, and processes.

Audience

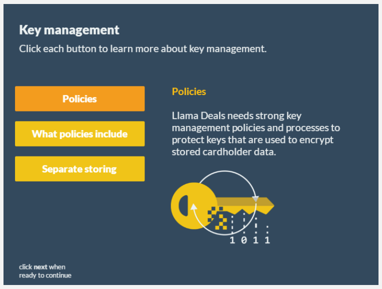
Developers
General Staff

Time Required

Tailored learning - 40 minutes total



Unnecessary default accounts



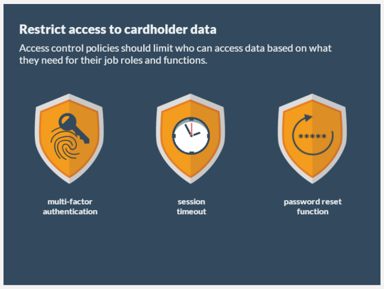
Key management

Click each button to learn more about key management.

Policies

Llama Deals needs strong key management policies and processes to protect keys that are used to encrypt stored cardholder data.

click **next** when ready to continue



Restrict access to cardholder data

Access control policies should limit who can access data based on what they need for their job roles and functions.

Security Compass

PCI101 - PCI-DSS Compliance

Course Outline

1. An intro to PCI-DSS

- What is PCI-DSS compliance?
- What is cardholder data?
- What is sensitive authentication data?
- What is the cardholder data environment?
- Optional quiz
- Who does PCI-DSS apply to?
- What CDE can include?
- What are the 12 requirements of PCI-DSS?
- What does the 12 requirements achieve?
- Newsflash: Equifax data breach
- Myths and facts
- Summary

2. Data protection

- Protect stored cardholder data
- Protect stored cardholder data - Best practices
- Newsflash: Orbitz Data Breach
- Encrypt stored cardholder data
- Key management
- Secure storing
- Key management procedures
- Encrypt transmission of cardholder data
- Restrict access to cardholder data
- Identify and authenticate access to system components
- Restrict physical access to cardholder data
- Restrict physical access to cardholder data - in practice
- Create and maintain an information security policy
- Service providers
- Documentation
- Summary

3. Network security

- Firewall configuration
- Firewall configuration - details
- Vendor-supplied defaults and other security parameters
- Unnecessary default accounts
- Access to network resources and cardholder data
- Precautions
- Test security
- Malware and viruses
- Systems and applications
- Change control processes and procedures
- Implement changes
- Summary

Security Compass