PCI – DSS
Requirements

12

REQUIREMENTS

- Information Security
- Secure Network
- Secure Card Holder Data
- Vulnerability Management
- Access Control
- Network Monitoring And Testing

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.

3. Protect stored cardholder data.

4. Encrypt transmission of cardholder data across open public networks.

5. Use and regularly update anti-virus software or programs.

6. Develop and maintain secure systems and applications.

7. Restrict access to cardholder data by business need to know.

8. Assign a unique ID to each person with computer access.

9. Restrict physical access to cardholder data.

10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

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

Thank you!

Like, subscribe, follow (why not all 3?)

- ✓ Auditing of financial and systems
- ✓ Cloud awareness
- ✓ Certified Information Systems Audits

@Chidambaram-narayanan