InfoShield

PCI DSS Compliance

November 13, 2018

PCI

Thinking of taking payments at your business? Before taking and storing credit cards there are some regulations you're required to comply with or you could risk fines passed down from your merchant account, increased percentage costs per transaction, or possibly even losing the merchant account entirely. These 12 items are a starter to putting you on path to avoiding these pitfalls.

PCI DSS Compliance Checklist

by **Josh Susen, CISSP**

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 anti-virus 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

https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1542157937368

Get more help from us

Other Resources and Further Reading

https://www.pcisecuritystandards.org

Infoshield is an IT Security Consulting Company

Fernandina Beach, FL