5NINES CYBER SECURITY SERVICES

PCI DSS REQUIRED COMPLIANCE

WHAT IS PCI DSS?

The Payment Card Industry Data Security Standard is a set of information security standards for organizations that handle branded credit, debit and cash cards. It's designed to protect the safety of customer data and it's required for all entities that store, process or transmit cardholder data.

WHO DOES IT APPLY TO?

PCI DSS compliance includes all entities that store, process or transmit cardholder data:

- Merchants of all sizes
- Financial institutions
- Point-of-sale vendors
- Hardware and software developers

WHY TO COMPLY?

Compliance with PCI-DSS is required by law and implies violation fines ranging from $5,000 to $100,000 per month by the credit card company.

Potential Liabilities*:

- Lost confidence, so customers go to other merchants
- Diminished sales
- Cost of reissuing new payment cards
- Fraud losses
- Higher subsequent costs of compliance
- Legal costs, settlements and judgments
- Fines and penalties
- Termination of ability to accept payment cards
- Lost jobs (CISO, CIO, CEO and dependent professional positions)
- Going out of business

*https://www.pcisecuritystandards.org/pci_security/why_security_matters

HOW CAN 5NINES HELP YOU?

5NINES is a proud member of Cloud Security Alliance and a partner of WMEP and WICMP. We provide a full range of cyber security services from vulnerability assessment to AOC certification and employee training.

- Onsite and Offsite security assessments and full report on PCI compliance (ROC)
- Assistance with Self Assessment procedures and reporting (SAQ)
- Assistance with Attestation of Compliance (AOC) certificate
- Risk Assessment
- Network Penetration Testing
- Vulnerability Scanning
- Security Awareness and Training services

OUR CYBERSECURITY SERVICE & PRICING

1	COMPREHENSIVE VULNERABILITY ASSESSMENT (CVA).....	$5000*
2	MITIGATION PLAN.....	Call for pricing*
3	MANAGED SERVICES.....	Call for pricing*

*Applies to one location and off-site storage

5NINES LLC I 316 West Washington Avenue, Suite 600 I Madison, WI 53703 I 608.512.1000 I inquiry@5nines.com

PCI SECURITY STANDARDS

Maintaining the safety of your client data is crucial whether you are a small business owner or a big company manager. 5NINES can help you understand, follow the requirements and fully comply with PCI DSS.

GOALS	PCI DSS REQUIREMENTS
Build and Maintain a Secure Network	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. Use 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. Assign a unique ID to each person with computer access 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 employees and contractors

https://www.pcisecuritystandards.org/merchants/process

HOW TO COMPLY WITH PCI DSS

PCI Security Standards Council identifies the following steps of the compliance process:

1. **Scope**-determine which system components and networks are in scope for PCI DSS
2. **Assess** -examine the compliance of system components in scope following the testing procedures for each PCI DSS requirement
3. **Report** - assessor and/or entity completes required documentation (e.g. Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls
4. **Attest**- complete the appropriate Attestation of Compliance (AOC)
5. **Submit** - submit the SAQ, ROC, AOC and other requested supporting documentation such as ASV scan reports to the acquirer (for merchants) or to the payment brand/requestor (for service providers)
6. **Remediate** – if required, perform remediation to address requirements that are not in place, and provide an updated report

WHAT WE OFFER?

1. Comprehensive Vulnerability Assessment (CVA)

- First step in addressing security vulnerabilities
- Identifies next steps

2. Remediation

- Address and correct each vulnerability

3. Managed Services

- Evaluate your needs, order, update, install and maintain systems within your budget and on your timeline

4. Ongoing Assessments

- Ensures you maintain compliance as time goes on

Visit our website for more information at security.5nines.com

5NINES LLC I 316 West Washington Avenue, Suite 600 I Madison, WI 53703 I 608.512.1000 I inquiry@5nines.com