THE NATIONAL CYBERSECURITY SOCIETY

PCI-DSS

PCI-DSS (Payment Card Industry Data Security Standard) Compliance

The Payment Card Industry Data Security Standard is an information security standard for organizations that handle credit cards from the major card companies. The standards are maintained by the PCI-DSS Council, and establish the controls necessary to protect from credit card fraud. A qualified auditor asserts compliance for organizations that process large transaction volume, and businesses that handle smaller volumes (less than 6 million) can assess their compliance through a self-assessment questionnaire. The standards apply to organizations that accept payment for goods and/or services from **any** of the five members of the council – American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.

Compliance assertion covers two important activities: 1) completing the applicable self-assessment questionnaire and 2) attesting to compliance. This tip guide covers the 12 elements of PCI-DSS (policies and procedures), which are needed to ensure compliance.

DID YOU KNOW?

- ✓ Buy and use only validated payment software for your point of sale system and website shopping cart.
- ✓ Teach your employees about protecting cardholder data.
- ✓ Do **NOT** store sensitive cardholder data on computers or on paper.
- ✓ Ensure your wireless router is password protected and encrypted.
- ✓ The twelve PCI-DSS standards are best practices for all businesses, not just merchants.

TIP 1: FIREWALL AND ROUTER CONFIGURATIONS

PCI-DSS #1 is about protecting access to cardholder data and assesses an organization's firewall and router configurations to ensure data protections are in place to protect cardholder data.

TIP 2: VENDOR SUPPLIED DEFAULTS

PCI-DSS #2 requires vendor-supplied defaults for system passwords are changed from the default password provided by the manufacturer (such as wireless router). Includes a review of the security policies and procedures for managing vendor defaults and other security parameters to determine if the policy is documented, in-use and known to all affected parties.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

PCI-DSS continued...

TIP 3: STORED CARDHOLDER DATA

PCI-DSS #3 ensures stored cardholder data is encrypted while stored and during transit and that the three-digit verification code is not stored after authorization is complete.

TIP 4: TRANSMISSION OF CARDHOLDER DATA

PCI-DSS #4 requires the transmission of cardholder data across open, public networks is encrypted. Also requires that stored cardholder data is encrypted and that the three-digit verification code is not stored after authorization is complete.

TIP 5: ANTI-VIRUS AND MALWARE PROTECTION

PCI-DSS #5 states that all systems will be protected against malware and that anti-virus software is installed and kept up to date. Since malware is often deployed on systems through clicking on links, opening attachments, educating employees about this theft is crucial.

TIP 6: PATCH AND CORRECT VULNERABILITIES

PCI-DSS #6 addresses scanning and identifying vulnerabilities in an organization's IT infrastructure (see our fact sheet on Vulnerability Assessments). Installing up-to-date of software and avoiding insecure implementations are two areas critical to ensuring compliance with PCI-DSS #6.

TIP 7: RESTRICT ACCESS

PCI-DSS #7 requires the business to restrict access to cardholder data. Only employees with a bona-fide need should have access to systems that store or transmit cardholder data.

TIP 8: ASSIGN UNIQUE ID TO USERS

PCI-DSS #8 requires a user name and password be assigned to all users of the systems that hold cardholder data. Users accessing systems that hold cardholder data should be promoted to provide identity credentials (user name) password to authenticate access to system components. Passwords should be updated regularly (every 90 days), follow strong password construction rules, and have lockouts if multiple attempts are exercised.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

PCI-DSS continued…

TIP 9: RESTRICT PHYSICAL ACCESS

PCI-DSS #9 requires the business to restrict **physical** access to cardholder data. Ensure the facility where the point sale, wireless router and cardholder data storage has physical controls to prevent access such as locks or safes. Ensure procedures or devices (such as cameras) are in place to monitor the facility or devices to verify whether a compromise might have occurred during non-duty hours.

TIP 10: TRACK AND MONITOR ACCESS TO RESOURCES

PCI-DSS #10 Track and monitor access to all system resources – ensure the system storing cardholder data has an audit mechanism to determine if unauthorized access was attempted.

TIP 11: REGULARLY TEST SECURITY SYSTEMS

PCI-DSS #11 – Regularly (annually) test security systems; conduct penetration testing; vulnerability assessments; and ensure incident plan(s) in place. Compromised cardholder data constitutes a data breach and detailed processes are required to notify affected cardholders. Regularly review processes for data breach notification.

TIP 12: INFORMATION SECURITY FOR EMPLOYEES/CONTRACTORS

PCI-DSS #12 Publish your company's security policy and train all employees and contractors on how to protect cardholder data. Hold employees accountable for violating policy. Ensure any third party contractors (such as hosting providers) have incident and mitigation plans. Read the fine print of the SLA, and remember that you, the merchant, are responsible for protecting cardholder data even though it might be stored at an offsite provider.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.