Lewis Creek Systems, LLC

Payment Card Information Security

As of December, 2005 all merchants and service providers who handle credit card information are required to meet a new, common standard for information security, called the **Payment Card Industry (PCI) Data Security Standard**. How you are required to validate your compliance depends on how much business you do by payment card and whether or not you previously have suffered a breach of cardholder information.

If you suffer a breach and aren't in compliance, you could be **fined from $50,000 to $500,000** and be required to regularly conduct expensive third-party audits of your information security.

In order to be in compliance with the PCI Data Security Standard you need to satisfy **twelve basic requirements** in information security, as well as the many details that support those requirements.

Have you reviewed the security of your handling of cardholder information? Have you conducted a self-assessment or hired a qualified third party to assess how well you meet the 12 requirements of the PCI standard? Will you be ready to face the auditors and pay the fines if you suffer a breach of cardholder information?

Lewis Creek Systems is experienced in helping its clients comply with information security regulations and providing the information, tools, and services necessary to maintain the security of individual information and protect clients from the significant costs of cardholder information security breaches.

What are the 12 Requirements of the PCI Standard?

Each of the 12 requirements has sub-requirements defined in the PCI validation template. For instance, requirement 3 alone has 21 separate issues listed that must be satisfied during an audit or assessment. The twelve requirements are:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect Stored Data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each computer user
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

How can Lewis Creek Systems help?

1) The first step in reaching compliance with PCI security requirements is to perform a **detailed assessment of information flows** and **analysis of risk exposures** for all cardholder information.

2) **Technological or physical measures** can be taken to reduce risk exposures and **policies and procedures** can be implemented to meet the extensive requirements in the standard audit as well as address the risks exposed in the analysis.

3) Once new policies, procedures, and practices are established, **workforce training** may be conducted promote the necessary organizational **culture of privacy and security**.

Lewis Creek Systems has the experience to assist merchants and service providers in all of these critical tasks. **Specifically, we can help by providing:**

- **Training in Compliance Methods such as Information Flow and Risk Analysis**
- **Project Management Services**
- **Information Flow and Risk Analysis**
- **Technical Risk Evaluation Services**
- **Risk Determination Assistance**
- **Documentation of Systems and Processes**
- **Policy and Procedure Development**
- **PCI Security Compliance Reviews**
- **Documentation of Compliance Activities**
- **Workforce Security Training and Awareness Products and Services**

For more information…

Contact Steven Schaffer, Business Development Manager, at 203-254-1774.