17. Software Development Secure Coding Guidelines and Training Policy

Overview
In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Administrative Systems PCI Compliance Services has established a formal policy and supporting procedures concerning software development and secure coding guidelines and training. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Administrative Systems PCI Compliance Services’ needs and goals.

Policy
Administrative Systems PCI Compliance Services will ensure that the software development and secure coding guidelines and training policy and procedures adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.0):

- Software developers and all other relevant personnel involved in the development of software for payment applications per PCI standards are required to undergo annual training in secure coding techniques for the software platforms(s) with which they work.
- Software developers and all other relevant personnel involved in the development of software for payment applications per PCI standards are required to submit their Secure Coding Training checklist on an annual basis as evidence that they are knowledgeable in secure coding techniques.
- Software developers involved in the software development process will adhere to professional guidelines, such as the Open Web Application Security Project (OWASP) Code of Ethics and CWE/SANS.
- Administrative Systems PCI Compliance Services’s software development lifecycle includes policies, processes and procedures to ensure that internally-developed applications are not vulnerable to the following threats:
  - Injection Flaws (SQL, OS and LDAP Injection)
  - Buffer Overflows
  - Insecure Cryptographic Storage
  - Insecure Communications
  - Improper Error Handling
  - All high risk vulnerabilities identified in the vulnerability identification process as found in the Risk Ranking Table within the Security Patch Management Installation Policy and Procedures document.
  - Cross-Site Scripting
  - Improper Access Control
  - Cross Site Request Forgery
• Broken Authentication and Session Management
• All "High" vulnerabilities and threats as identified in the Risk Ranking Table found in the Security Patch Management Installation Policy and Procedures

Source: http://www.owasp.org

Responsibility for Policy Maintenance
Administrative Systems PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.