Policy Solution Table for Payment Card Industry (PCI) Data Security Standard*

Is your organization in need of a security policy program to address PCI compliance? The PCI Standards Council publishes a self-assessment guide to allow organizations to determine their level of compliance with PCI data protection requirements. A key section of the standard is **Requirement 12: Maintain a policy that addresses information security**. The following table demonstrates how the security policy requirements of the Payment Card Industry Data Security Standard can be addressed by Information Shield products including *Information Security Policies Made Easy, Version 10* (ISPME) and *Information Security Roles and Responsibilities Made Easy*, Version 2.0. (ISR&R)

Security Policy Program Requirements	**Information Shield Solution**
Requirement 12: Maintain a policy that addresses information security.	
12.1 Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?	ISPME contains over 1500 individual pre-written security policies covering 123 different security topics as defined in ISO 17799:2005 (ISO 27002). ISPME also contains 15 complete security policy documents covering key aspects of information security.
12.2 Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?	ISPME contains over 100 separate information security policy controls that relate to outsourcing and third-party contracts
12.3 Are information security policies reviewed at least once a year and updated as needed?	ISPME helps organizations maintain an updated set of written policies by providing content updates with each new version. ISPME also provides time-saving tutorials on the policy development and review cycle from Charles Cresson Wood, CISSP, CISA
12.4 Have the roles and responsibilities for information security been clearly defined within the company?	Information Security Roles and Responsibilities Made Easy provides over 70 different pre-written information security related job descriptions and department mission statements, allowing organizations to quickly document roles and responsibilities. ISR&R also includes time-saving tools and techniques for developing an information security program.
12.5 Is there an up-to-date information security awareness and training program in place for all system users?	ISPME contains pre-written policies that allow organizations to document and develop and information security awareness program. ISPME contains over 1500 policy commentaries with detailed advice that can help drive awareness activities.
12.6 Are employees required to sign an agreement verifying they have read and understood the security policies and procedures?	ISPME comes with pre-written information security policies that document the responsibilities and rights of users, including a sample Agreement to Comply with Information Security Policies.
12.7 Is a background investigation (such as a credit- and criminal record check, within the limits of local law) performed on all employees with access to account numbers?	ISPME contains over 100 different pre-written information security policies covering the entire lifecycle of employee management, including pre-screening, during employment, and after termination.

12.8 Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?	ISPME contains over 100 different information security controls relating the management of security with outsourcing contracts and third party access to sensitive information.
12.9 Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?	ISPME contains over 80 different information security policies covering each aspect of incident reporting, management, handling and disclosure.
12.10 Are security incidents reported to the person responsible for security investigation?	ISPME contains pre-written policies for the reporting and documentation of security incidents.
12.11 Is there an incident response team ready to be deployed in case of a cardholder data compromise?	ISPME contains pre-written policies for the formation and documentation of a Computer Incident Response Team (CIRT), while ISR&R provides specific pre-written job responsibilities and mission statements for members of a Computer Incident Response Team.

**Based on the Payment Card Industry (PCI) Data Security Standard, Self-Assessment Questionnaire Version 1.2, Release: October 2008, available from the PCI Standards Council.*

For more information a security policy solutions for PCI compliance visit our Regulatory Resource Center at http://www.informationshield.com