Appendix A: PCI DSS Mapping

|  |  |  |
| --- | --- | --- |
| Mapping between PCI DSS Requirements and ISPL | | |
| **Req #** | **Requirement** | **ISPL Document** |
| 1 | **Secure network and systems** |  |
| 1.1 | Firewall and router configuration standards; identify all connections to cardholder data; network diagram; data flows for cardholder data; configuration review every 6 months; testing after configuration change | Network Configuration Standards IT Change Management Procedure Firewall Configuration Change From |
| 1.2 | Deny all inbound and outbound traffic to cardholder data network; allow only that which is required | Network Configuration Standards |
| 1.3 | Prevent direct traffic from the Internet to the CDE | Network Configuration Standards |
| 1.4 | Personal firewall on any mobile or employee-owned devices | PCI Compliance Policy |
| 1.5 | Related security policies documented, in use, and known to affected parties | Information Security Policy |
| **2** | **Do not use vendor defaults for passwords and other security parameters** |  |
| 2.1 | Always change vendor defaults, and remove unnecessary accounts, including wireless devices | Password Policy Network Configuration Standard |
| 2.2 | Configuration standards for all components to address known vulnerabilities; update configurations as new vulnerabilities are discovered. | Network Configuration Standard |
| 2.3 | Encrypt all non-console admin traffic using strong cryptography | Data Encryption Policy |
| 2.4 | Maintain an inventory of all components in scope for PCI DSS | PCI Compliance Policy |
| 2.5 | Related security policies documented, in use, and known to affected parties |  |
| **3** | **Protect stored Cardholder Data** |  |
| 3.1 | Limit CD stored to the amount needed, and the retention time required; purge unnecessary data at least quarterly. | PCI Compliance Policy |
| 3.2 | Do not store sensitive authentication data | PCI Compliance Policy |
| 3.3 | Mask PAN when displayed; limit full display to essential personnel. | PCI Compliance Policy |
| 3.4 | Render PAN unreadable when stored. | PCI Compliance Policy |
| 3.5 | Procedures to protect keys used for encryption from disclosure and misuse. | Data Encryption Policy |
| 3.6 | Fully document key management processes | Data Encryption Policy |
| 3.7 | Related security policies documented, in use, and known to affected parties |  |
| **4** | **Encrypt transmission of CHD across open, public networks** |  |
| 4.1 | Use strong cryptography and security protocols when transmitting CHD across open, public networks; Use industry best practices. | Data Encryption Policy |
| 4.2 | Never send PAN via end-user messaging (email, SMS, etc) | Data Encryption Policy |
| 4.3 | Related security policies documented, in use, and known to affected parties |  |
| **5** | **Protect all systems against malware, and regularly update anti-virus software** |  |
| 5.1 | Deploy anti-virus software on all systems subject to malware | Acceptable Use Policy |
| 5.2 | Ensure that anti-virus mechanisms are kept current | Acceptable Use Policy |
| 5.3 | Ensure that anti-virus mechanisms are actively running, and cannot be disabled by users | Acceptable Use Policy |
| 5.4 | Related security policies documented, in use, and known to affected parties |  |
| **6** | **Develop and maintain secure systems and applications** |  |
| 6.1 | Identify security vulnerabilities using a reputable outside source; assign a risk ranking. | System Acceptance and Configuration Policy |
| 6.2 | Install applicable vendor-supplied security patches; install critical patches within one month. | System Patching Policy |
| 6.3 | Securely develop internal and external software applications in accordance with PCI requirements and industry best practices |  |
| 6.4 | Follow change control processes/procedures for all changes to system components. | IT Change Management Procedure |
| 6.5 | Prevent common coding vulnerabilities by training developers in secure coding techniques |  |
| 6.6 | Protect public-facing web applications by application assessments quarterly of after changes, or using automated means | Vulnerability Management Policy |
| 6.7 | Related security policies documented, in use, and known to affected parties |  |
| **7** | **Restrict access to CHD to those with a need to know** |  |
| 7.1 | Limit CHD access to those who require such access to do their jobs | PCI Compliance Policy |
| 7.2 | Establish access control system; set to deny all, unless specifically required | PCI Compliance Policy |
| 7.3 | Related security policies documented, in use, and known to affected parties |  |
| **8** | **Identify and authenticate access to system components** |  |
| 8.1 | Policies and procedures to ensure proper user identification management, including unique user names | PCI Compliance Policy |
| 8.2 | Employ at least one to authenticate all users: 1) Something you know; 2) Something you have; 3) Something you are. | User Account Management Policy |
| 8.3 | Use two-factor authentication for all remote access. | Remote Access Policy |
| 8.4 | Develop, implement, and communicate authentication policies and procedures to all users. |  |
| 8.5 | Do not use group, shared, or generic user ids | PCI Compliance Policy |
| 8.6 | Use of authentication methods, such as tokens, must be assigned to specific user ids | PCI Compliance Policy |
| 8.7 | Access to databases containing CHD must be restricted; only DBAs may have direct query access | PCI Compliance Policy |
| 8.8 | Related security policies documented, in use, and known to affected parties |  |
| **9** | **Restrict physical access to CHD** |  |
| 9.1 | Use facility entry controls to restrict and track access to systems with CHD | PCI Compliance Policy |
| 9.2 | Use ID badges or other means to distinguish visitors from employees. | Physical and Environmental Security Policy |
| 9.3 | Control physical access by employees based on job function; revoke access immediately upon termination. | Physical and Environmental Security Policy |
| 9.4 | Ensure that visitors are authorized before entering areas with CHD; use tokens to identify that expire and are revoked when leaving; use a visitor log, and retain for at least 3 months. | Physical and Environmental Security Policy |
| 9.5 | Physically secure media; store backups securely, preferably offsite. | Backup and Recovery Policy |
| 9.6 | Strictly control media distribution. | IT Asset Accountability Policy |
| 9.7 | Strictly control media storage and accessibility. | Backup and Recovery Policy |
| 9.9 | Protect devices with interact with cards from tampering and substitution; periodically inspect POS devices; train personnel to spot suspicious activity. | PCI Compliance Policy |
| 9.10 | Related security policies documented, in use, and known to affected parties |  |
| **10** | **Track and monitor all access to network resources and CHD** |  |
| 10.1 | Implement audit trails to link access attempts to each individual user. | User Account Management Policy |
| 10.2 | Implement audit trails to all reconstruction of key events, such as access by an individual with admin access | User Account Management Policy |
| 10.3 | Record for each event the user id, type of event, date/time, success/failure, origination, name/identity of system or resource | System Logging and Monitoring Policy |
| 10.4 | Synchronize time clocks | System Logging and Monitoring Policy |
| 10.5 | Secure audit trails so they cannot be altered | System Logging and Monitoring Policy |
| 10.6 | Review logs and security events; perform critical log reviews daily. | System Logging and Monitoring Policy |
| 10.7 | Retain audit trails for one year, with three months readily available | System Logging and Monitoring Policy |
| 10.8 | Protect devices with interact with cards from tampering and substitution; periodically inspect POS devices; train personnel to spot suspicious activity. | PCI Compliance Policy |
| **11** | **Regularly test security systems and processes** |  |
| 11.1 | Inventory and test for wireless access points | Network Configuration Standard |
| 11.2 | Run internal and external network vulnerability scans quarterly, and after a significant change; quarterly scans must be done by an ASV; correct issues and re-run scans until clean | Vulnerability Management Policy |
| 11.3 | Run penetration scans at least annually, and after a major change; test network segmentation designed to reduce PCI scope | Vulnerability Management Policy |
| 11.4 | Use IDS/IPS to detect and prevent network intrusions | Network Configuration Standard |
| 11.5 | Implement a change detection methodology, such as file integrity monitoring | Physical and Environmental Security Policy |
| 11.6 | Related security policies documented, in use, and known to affected parties |  |
| **12** | **Maintain a policy that addresses information security for all personnel** |  |
| 12.1 | Establish, maintain, and publish a security policy; update manually, or after significant changes | Information Security Policy |
| 12.2 | Implement a risk assessment process, performed at least annually | IT Risk Management Policy |
| 12.3 | Implement an acceptable use policy for critical technologies, such as laptops, remote access, etc | Acceptable Use Policy |
| 12.4 | Ensure that the security policy and procedures clearly define information security responsibilities for all personnel | Information Security Policy |
| 12.5 | Assign information security responsibilities to an individual or group | Information Security Policy |
| 12.6 | Implement a formal security awareness program | Cybersecurity Awareness Training Policy |
| 12.7 | Screen candidates prior to hiring | Personnel Security Policy |
| 12.8 | Implement a program to manage service providers with access to PCI data | PCI Compliance Policy |
| 12.9 | N/A |  |
| 12.10 | Implement an incident response plan | Incident Management Policy |