PCI Compliance & Server General

Section	PCI DSS Requirement	Server General	
2.1	Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	√	
2.2.1	Implement only one primary function per server.	√	
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).	√	
2.2.3	Configure system security parameters to prevent misuse.	√	
2.2.4	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	√	
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	√	
3.4	Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches: § One-way hashes based on strong cryptography § Truncation § Index tokens and pads (pads must be securely stored) § Strong cryptography with associated key-management processes and procedures The MINIMUM account information that must be rendered unreadable is the PAN.	√	
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	√ [1]	
3.4.1.b	Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).	√ [5]	
3.4.1.c	Verify that cardholder data on removable media is encrypted wherever stored.	√ [5]	

3.5	Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:	√	
3.5.1	Restrict access to cryptographic keys to the fewest number of custodians necessary.	√	
3.5.2	Store cryptographic keys securely in the fewest possible locations and forms.	√	
3.6.1	Generation of strong cryptographic keys	√	
3.6.2	Secure cryptographic key distribution	√	
3.6.3	Secure cryptographic key storage	√	
3.6.4	Periodic cryptographic key changes - As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically - At least annually	√	
3.6.5	Retirement or replacement of old or suspected compromised cryptographic keys	√	
3.6.6	Split knowledge and establishment of dual control of cryptographic keys.	√	
3.6.7	Prevention of unauthorized substitution of cryptographic keys	√	
4.1	Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.	√	
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	√ [2]	
6.2	Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	√ [2]	
6.2.b	Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2.2 as new vulnerability issues are found.	√ [2] [5]	
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:		

7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	√ [3]	
7.1.2	Assignment of privileges is based on individual personnel's job classification and function	√ [3]	
7.1.4	Implementation of an automated access control system	√	
8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	√	
8.2	In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: § Password or passphrase § Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	√	
8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:		
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	√	
8.5.2	Verify user identity before performing password resets.	√	
8.5.4	Immediately revoke access for any terminated users.	√	
8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed.	√	
8.5.9	Change user passwords at least every 90 days.	√	
8.5.10	Require a minimum password length of at least seven characters.	√	
8.5.11	Use passwords containing both numeric and alphabetic characters.	√	
8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	√	
10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	√	

10.2	Implement automated audit trails for all system components to reconstruct the following events:		
10.2.2	All actions taken by any individual with root or administrative privileges	√	
10.2.4	Invalid logical access attempts	√	
10.2.7	Creation and deletion of system-level objects	√	
10.3	Record at least the following audit trail entries for all system components for each event:		
10.3.1	User identification	√	
10.3.2	Type of event	√	
10.3.3	Date and time	√	
10.3.4	Success or failure indication	√	
10.3.5	Origination of event	√	
10.3.6	Identity or name of affected data, system component, or resource	√	
10.4	Synchronize all critical system clocks and times.	√	
10.5	Secure audit trails so they cannot be altered.	√	
10.5.1	Limit viewing of audit trails to those with a job-related need.	√	
10.5.2	Protect audit trail files from unauthorized modifications.	√	
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	√	
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	√	
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	√	

[1] Logical access control is used even though disk encryption is not used.

[2] Server General provides a security update service (comes bundled with the solution).
[3] Server General solutions use RBAC
[4] Smart-cards are used for two factor authentication as well as for key management.
[5] In order to clarify the mandate, the language of this mandate has been substituted by the corresponding "test procedure" recommended by the PCI council.
[6] Server General doesn't store the encryption key anywhere.
[7] Server General uses soft tokens.

Note#1: The red characters indicate a strong match between a built-in product feature and a PCI mandate.

Note#2: The broad headings "7.1", "8.5", "10.2", "10.3" are listed without check marks, because the sub-mandates of each heading are intended to address the directives accordingly.