

Payment Card Industry (PCI) Data Security Standard

Self-Assessment Questionnaire
(Version 1.0, Release: December 2004)

Bsafe PCI Compliance For System i (iseries / AS400), System z (z/OS, VSE & MVS)

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

DESCRIPTION		RESPONSE		
1.1	Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
1.2	If wireless technology is used, is the access to the network limited to authorized devices? (By IP address)	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
1.3	Do changes to the firewall need authorization and are the changes logged?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
1.4	Is a firewall used to protect the network and limit traffic to that which is required to conduct business?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
1.5	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
1.6	Is payment card account information stored in a database located on the internal network (not the DMZ) and protected by a firewall?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
1.7	If wireless technology is used, do perimeter firewalls exist between wireless networks and the payment card environment?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
1.8	Does each mobile computer with direct connectivity to the Internet have a personal firewall and anti-virus software installed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
1.9	Are Web servers located on a publicly reachable network segment separated from the internal network by a firewall (DMZ)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
1.10	Is the firewall configured to translate (hide) internal IP addresses, using network address translation (NAT)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	

Supported by Bsafe/ES Modules:

- Bsafe Network IPS (firewall)

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

DESCRIPTION		RESPONSE		
2.1	Are vendor default security settings changed on production systems before taking the system into production?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
2.2	Are vendor default accounts and passwords disabled or changed on production systems before putting a system into production?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
2.3	If wireless technology is used, are vendor default settings changed (i.e. WEP keys, SSID, passwords, SNMP community strings, disabling SSID broadcasts)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
2.4	If wireless technology is used, is Wi-Fi Protected Access (WPA) technology implemented for encryption and authentication when WPA-capable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
2.5	Are all production systems (servers and network components) hardened by removing all unnecessary services and protocols installed by the default configuration?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
2.6	Are secure, encrypted communications used for remote administration of production systems and applications? (In the presence of an SSL support)	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Supported by Bsafe/ES Modules:

- Bsafe Policy Compliance
- Bsafe Policy Templates
- System Default Policy

Protect Cardholder Data

Requirement 3: Protect stored data

DESCRIPTION		RESPONSE	
3.1	Is sensitive cardholder data securely disposed of when no longer needed?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
3.2	Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or point-of-sale products?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
3.3	Is it prohibited to store the card-validation code (three-digit value printed on the signature panel of a card) in the database, log files, or point-of-sale products?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
3.4	Are all but the last four digits of the account number masked when displaying cardholder data?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
3.5	Are account numbers (in databases, logs, files, backup media, etc.) stored securely— for example, by means of encryption or truncation?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
3.6	Are account numbers sanitized before being logged in the audit log?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

DESCRIPTION		RESPONSE		
4.1	Are transmissions of sensitive cardholder data encrypted over public networks through the use of SSL or other industry acceptable methods?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
4.2	If SSL is used for transmission of sensitive cardholder data, is it using version 3.0 with 128-bit encryption?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.3	If wireless technology is used, is the communication encrypted using Wi-Fi Protected Access (WPA), VPN, SSL at 128-bit, or WEP?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
4.4	If wireless technology is used, are WEP at 128-bit and additional encryption technologies in use, and are shared WEP keys rotated quarterly?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.5	Is encryption used in the transmission of account numbers via e-mail?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Supported by Bsafe/ES Modules:

- Bsafe Encryption (from Disuk)
- Bsafe Field Masking
- SSL IBM Crypto

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

	DESCRIPTION	RESPONSE
5.1	Is there a virus scanner installed on all servers and on all workstations, and is the virus scanner regularly updated?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Requirement 6: Develop and maintain secure systems and applications

	DESCRIPTION	RESPONSE
6.1	Are development, testing, and production systems updated with the latest security-related patches released by the vendors?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
6.2	Is the software and application development process based on an industry best practice and is information security included throughout the software development life cycle (SDLC) process?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
6.3	If production data is used for testing and development purposes, is sensitive cardholder data sanitized before usage?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
6.4	Are all changes to the production environment and applications formally authorized, planned, and logged before being implemented?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
6.5	Were the guidelines commonly accepted by the security community (such as Open Web Application Security Project group (www.owasp.org)) taken into account in the development of Web applications?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A
6.6	When authenticating over the Internet, is the application designed to prevent malicious users from trying to determine existing user accounts?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
6.7	Is sensitive cardholder data stored in cookies secured or encrypted?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
6.8	Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

Supported by Bsafe/ES Modules:

- Bsafe Network IPS
- Bsafe Field Masking
- Bsafe administration audit
- Bsafe Alerts
- Bsafe Encryption (by Disuk)
- Bsafe Authority Swap

Implement Strong Access Control Measures

Requirement 7: Restrict access to data by business need-to-know

	DESCRIPTION	RESPONSE	
7.1	Is access to payment card account numbers restricted for users on a need-to-know basis?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No

Requirement 8: Assign a unique ID to each person with computer access

	DESCRIPTION	RESPONSE		
8.1	Are all users required to authenticate using, at a minimum, a unique username and password?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
8.2	If employees, administrators, or third parties access the network remotely, is remote access software (such as PCAnywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8.3	Are all passwords on network devices and systems encrypted?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
8.4	When an employee leaves the company, are that employee's user accounts and passwords immediately revoked?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
8.5	Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
8.6	Are non-consumer accounts that are not used for a lengthy amount of time (inactive accounts) automatically disabled in the system after a pre-defined period?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
8.7	Are accounts used by vendors for remote maintenance enabled only during the time needed?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8.8	Are group, shared, or generic accounts and passwords prohibited for non-consumer users?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
8.9	Are non-consumer users required to change their passwords on a pre-defined regular basis?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
8.10	Is there a password policy for non-consumer users that enforces the use of strong passwords and prevents the resubmission of previously used passwords?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
8.11	Is there an account-lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	

Supported by Bsafe/ES Modules:

- Bsafe Network IPS
- Bsafe Authority Swap
- Bsafe tokens (by Vaseo)
- Bsafe Inactive users
- Bsafe Audit & Alerts
- Bsafe Policy Compliance
- Bsafe Profile Manager
- Bsafe Analyzer

Requirement 9: Restrict physical access to cardholder data

DESCRIPTION		RESPONSE		
9.1	Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
9.2	If wireless technology is used, do you restrict access to wireless access points, wireless gateways, and wireless handheld devices?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
9.3	Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
9.4	Is all cardholder data printed on paper or received by fax protected against unauthorized access?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
9.5	Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	
9.6	Are all media devices that store cardholder data properly inventoried and securely stored?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
9.7	Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

DESCRIPTION		RESPONSE	
10.1	Is all access to cardholder data, including root/administration access, logged?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
10.2	Do access control logs contain successful and unsuccessful login attempts and access to audit logs?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
10.3	Are all critical system clocks and times synchronized, and do logs include date and time stamp?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
10.4	Are the firewall, router, wireless access points, and authentication server logs regularly reviewed for unauthorized traffic?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
10.5	Are audit logs regularly backed up, secured, and retained for at least three months online and one-year offline for all critical systems?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No

Requirement 11: Regularly test security systems and processes

DESCRIPTION		RESPONSE		
11.1	If wireless technology is used, is a wireless analyzer periodically run to identify all wireless devices?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
11.2	Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
11.3	Is an intrusion detection or intrusion prevention system used on the network?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
11.4	Are security alerts from the intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored, and are the latest IDS/IPS signatures installed?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	

Supported by Bsafe/ES Modules:

- Bsafe Network Log
- Bsafe Analyzer
- Bsafe Traffic Analyzer
- Bsafe Archive Central Audit
- Bsafe Simulator
- Bsafe IDS (alerts)
- Bsafe IPS

Maintain a policy that addresses information security

Requirement 12: Maintain a policy that addresses information security

DESCRIPTION		RESPONSE		
12.1	Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
12.2	Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
12.3	Are information security policies reviewed at least once a year and updated as needed?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
12.4	Have the roles and responsibilities for information security been clearly defined within the company?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
12.5	Is there an up-to-date information security awareness and training program in place for all system users?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
12.6	Are employees required to sign an agreement verifying they have read and understood the security policies and procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
12.8	Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
12.9	Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A
12.10	Are security incidents reported to the person responsible for security investigation?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
12.11	Is there an incident response team ready to be deployed in case of a cardholder data compromise?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> N/A

Supported by Bsafe/ES Modules:

- Bsafe Policy Compliance