PCI Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

ABC Company values its relationships with our customers, service providers, and regulators. Managing compliance requirements helps us maximize our opportunities in the market, enhances our competitive position, and helps build trust.

# II. Purpose

The Payment Card Industry Data Security Standard is a proprietary information security standard for organizations that handle cardholder information. A strong compliance program provides our organization with a competitive advantage, helps protect our image and reputation, and reduces our costs.

# III. Scope

This policy applies to all ABC Company Staff who have access to or manage Information Resources that collect, transmit, process, or store customer payment card data.

# IV. Policy

The Payment Card Industry Data Security Standard (PCI DSS) was developed to increase controls around cardholder data. Its purpose is to reduce credit card fraud that occurs as a result of unauthorized disclosure. As outlined in the following table, PCI DSS specifies 12 requirements for compliance, organized into six logically related groups (control objectives).

|  |
| --- |
| **Control Objectives and PCI DSS Requirements** |
| Build and Maintain a Secure Network and Systems  1. Install and maintain a firewall configuration to protect cardholder data  2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data  3. Protect stored cardholder data  4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program  5. Protect all systems against malware and regularly update anti-virus software or programs  6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures  7. Restrict access to cardholder data by business need-to-know  8. Identify and authenticate access to system components  9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks  10. Track and monitor all access to network resources and cardholder data  11. Regularly test security systems and processes |
| Maintain an Information Security Policy  12. Maintain a policy that addresses information security for all personnel |

The IT Department shall document the flow of cardholder information. Such documentation shall consider the flow of information within ABC Company as well as with external third party service providers.

The IT Department shall identify all sources and uses of cardholder data and prepare network and data flow diagrams that identify where cardholder data is collected, transmitted, stored, processed, and archived. The IT Department shall include, but not be limited to, software applications, network infrastructure equipment (e.g. servers, storage), backup/recovery sites, fail-over systems, and other relevant devices. IT Department documentation shall identify how the cardholder data environment was determined.

The Chief Security Officer (CSO) shall ensure:

* The cardholder data environment identifies and documents the existence of all cardholder data and that no cardholder data exists outside of the defined environment. If cardholder data is found outside of the defined environment, the cardholder data should be securely deleted, migrated into the defined environment, or the defined environment should be expanded to include the additional cardholder data.
* Network segmentation is considered as a means of protecting the cardholder data environment. Network segmentation can be achieved through physical or logical controls that isolate and protect the cardholder data environment.
* Third party service providers validate compliance requirements by either having an assessment on their own providing sufficient evidence to customers or by participating in customer reviews of the service provider environment.
* Monitoring systems ensure security controls are operating effectively and as intended. Such controls include, but are not limited to, firewalls, intrusion detection and prevention systems (IDS/IPS), file integrity monitoring, anti-malware, and access controls. Failures in security controls shall be detected and responded to in a timely manner. Processes to respond to security control failures shall include restoring the security control, identifying the cause of failure, identifying and addressing any security issues that arose during the failure of the security control, implementing mitigating controls prevent the failure, and resuming monitoring of the security control.
* The cardholder data environment is periodically reviewed for changes and potential impact.
* Security controls are reviewed and updated as a result of changes in the organization or cardholder data environment.
* Periodic reviews are performed to confirm compliance with PCI requirements. Such reviews shall ensure that security controls are sufficient and effective at protecting the cardholder data environment. Documentation shall be retained as evidence of the reviews.
* Annual reviews of hardware and software are performed to confirm the environment is supported by the appropriate vendors and the environment meets applicable security requirements.
* Where possible, security and audit functions are separated from IT operations.
* Effective methods of data discovery are used to identify unencrypted cardholder data. Ensure response procedures are initiated upon the detection of unencrypted cardholder data.
* Data Loss Prevention (DLP) mechanisms detect and prevent unencrypted cardholder data from leaving the environment.

In addition to the above responsibilities, the CSO shall ensure:

* Configuration rule sets are reviewed by System Administrators at least every six (6) months.
* The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
* Verification codes or values (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions are not stored.
* Personal identification number (PIN) or the encrypted PIN block are not stored.
* Primary Account Number (PAN) is masked when displayed. The first six and last four digits are the maximum number of digits to be displayed.
* PAN is unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: One way hashes based on strong cryptography (hash must be of the entire PAN), Truncation (hashing cannot be used to replace the truncated segment of PAN, Index tokens and pads (pads must be securely stored), and strong cryptography with associated key management processes and procedures.
* Additional controls are in place when hashed and truncated versions of the same PAN are present in an environment.
* Only personnel with a legitimate business need can see the full Primary Account Number.
* Unprotected PANs are never sent by end-user messaging technologies (e.g. e-mail, instant messaging, chat, etc.).
* Devices that capture payment card data via direct physical interaction with the card are protected from tampering and substitution. Note: These requirements apply to card reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.
* An up-to-date list of devices is maintained. The list shall include make, model of device, location of device (e.g. address of the site or facility where the device is located), and device serial number or other method of unique identification
* Device surfaces shall be periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.
* Training is provided so personnel can be made aware of attempted tampering or replacement of devices. Training should include verification of the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices, Staff should not install, replace, or return devices without verification, Staff should be aware of suspicious behavior around devices (e.g. attempts by unknown persons to unplug or open devices), Staff should report suspicious behavior and indications of device tampering or substitution to appropriate personnel (e.g. to their manager or the CSO).
* Quarterly external vulnerability scans are performed via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.
* Older encryption protocols such as Wired Equivalent Privacy (WEP) or SSL are not used for authentication or transmission.
* Cardholder data storage is kept to a minimum, a Data Retention Policy and Disposal Policy exists, data storage and retention times are limited to that which is required for business, legal, and/or regulatory purposes, as documented in the Data Retention Policy.

The following data elements from the magnetic stripe, when properly secured, may be retained for business operations: Cardholder’s name, Primary Account Number, Expiration date, and service code.

The IT Department shall develop and maintain an inventory of all systems that store, process, and/or transmit cardholder data. At a minimum, the following information shall be maintained:

* Name – name of the system or device
* Data – cardholder data stored including field names
* Description – include reason for collecting, storing, use, or transmitting information
* Retention – time period that cardholder data is retained per ABC Company’s Data Retention Policy
* Security – protection measures including encrypting, masking, hashing, truncating data

The IT Department shall implement safeguards and controls to meet PCI Control Objectives and PCI DSS Requirements. Before wireless technology is implemented, an entity should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission. If wireless networks collect, store, process, and/or transmit cardholder data, the IT Department shall implement safeguards to protect the information. Such safeguards shall include:

* Defaults – change default passwords, service set identification (SSID) name
* Encryption – enable strong encryption (WPA or WPA2)
* Physical access – restrict physical access to wireless access points
* Logs – review and archive wireless log files per the Logging Policy and Data Retention Policy
* Usage – ensure use of wireless networks complies with Wireless Access Policy requirements

ABC Company policies and plans shall implement and maintain specific Safeguards to meet PCI compliance requirements.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff who have access to or manage Information Resources that collect, transmit, process, or store cardholder related data.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.07, MEA02.11, MEA03.01

GDPR Article 25, 32

HIPAA 164.312(a)(2)(iv), 164.312(c)(2)

ISO 27001:2013 A.9

NIST SP 800-37 3.1

NIST SP 800-53 IA-5

NIST Cybersecurity Framework ID.RA-6, PR.AC-1, DE.CM-1, RS.RP-1, RS.MI-2

PCI 1.1-5, 2.2-4, 2.6, 3.1-7, 4.1-3, 5.1-4, 6.1-6.2, 6.5, 6.6-7, 7.1-3, 8.1-8, 9.1-7, 9.9-10, 10.1-7, 10.8-9, 11.1-5, 11.6, 12.1-3, 12.5, 12.4-7, 12.8-11, A1, A2.1-3, A3.1-3, A3.2.1-6, A3.3.2