Encryption 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 information must be protected while stored and during transit. Encryption should be used to protect sensitive information.

# II. Purpose

The purpose of this policy is to provide guidance on the use of encryption to protect ABC Company’s information resources that contain, process, or transmit confidential information. Additionally, this policy provides direction to ensure that regulations are followed.

# III. Scope

This policy applies to all ABC Company Staff. It addresses encryption policy and controls for confidential data that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management.

# IV. Policy

The Chief Security Officer shall ensure:

* Policies, procedures, and processes identify sensitive information that should be encrypted to protect against persons or programs that have not been granted access.
* The organization has implemented a mechanism to encrypt and decrypt sensitive information whenever deemed appropriate. Procedures specify how the organization transmits sensitive information as well as how often the information is transmitted.
* Based on the Risk Analysis, when encryption is needed to protect sensitive information during transmission. Procedures specify the methods of encryption used to protect the transmission of sensitive information.
* Logical access is managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials) when disk encryption is used rather than file or column level database encryption.

A. Key lengths

ABC Company uses software encryption technology to protect confidential and other sensitive data. To provide the highest-level security while balancing throughput and response times, key lengths should be at least AES 256 bits for confidential data.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the ABC Company IT department.

B. Data at rest

Hard drives that are not fully encrypted, e.g., have encrypted partitions, virtual disks, or are unencrypted, but connect to encrypted USB devices, may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive’s unencrypted auto-recovery folder may retain files that have been saved to the encrypted portion of the disk or USB. Full disk encryption avoids this problem.

Confidential data at rest on computer systems owned by and located within ABC Company controlled spaces and networks should be protected by one or more of the following:

* Encryption
* Firewalls with strict access controls that authenticate the identity of those individuals accessing the data
* Sanitizing the data requiring protection during storage to prevent unauthorized exposure (e.g., truncating last four digits of a Primary Account Number).
* Other compensating controls including complex passwords, physical isolation/access, etc.

Using strong cryptography, all authentication credentials (i.e. passwords/phrases) shall be made unreadable during transmission and storage on all Information Systems.

Password protection should be used in combination with all controls including encryption. Password protection alone is not an acceptable alternative to protecting confidential information.

ABC Company secures its stored data on file systems, disks, and tape drives in servers and a Storage Area Network environment. All back up data is protected using AES 256-bit algorithm encryption methodologies.

Computer hard drives or other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure.

C. Portable Devices

Portable devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of confidential data are the result of stolen or lost Portable computing devices. The best way to prevent these exposures is to avoid storing confidential data on these devices. As a general practice, confidential data should not to be copied to or stored on a portable computing device or a non-ABC Company owned computing device. However, in situations that require confidential data to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

Each designated information resource owner shall identify information that is confidential. The information resource owner shall specify practices to include written authorization that verifies a legitimate business need for accessing and storing confidential information on a portable device and assesses the risk of unauthorized access to or loss of the data before granting permission for exceptions to this best practice.

All users must obtain specific permission from the data owner before storing confidential data on a portable computing device or a non-ABC Company owned computing device.

Hard drives of portable devices (laptops and personal digital assistants (PDAs) must be encrypted using products and/or methods approved by ABC Company‘s IT staff. Unless otherwise approved by IT management, such devices shall have full disk encryption with pre-boot authentication.

Portable devices should not be used for the long-term storage of any confidential information.

* Portable devices must have the proper protection mechanisms installed that include approved anti-malware software and firewall with unneeded services and ports turned off and properly configured applications.
* Removable media including CD’s, DVD’s, USB flash drives, etc. containing confidential information must be encrypted and stored in a secure, locked location. Such media must be transported in a secure manner.
* Portable or removable media that contain confidential data must be in the possession of the authorized user at all times (e.g., must not be checked as luggage while in transit).

ABC Company shall inventory encrypted devices and validate implementation of encryption products at least annually.

Data owners and users of portable computing devices and non-ABC Company owned computing devices containing confidential data must acknowledge how they ensure that data are encrypted and how encrypted data can be accessible by the owner in the event that an encryption key becomes lost or forgotten. Methods to meet this requirement include:

* Maintaining an accessible copy of the data.
* Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key.
* Escrowing the encryption key with a trusted party designated by the data owner and the ABC Company IT management.

D. Transmission Security

The Chief Security Officer (CSO) shall ensure:

* Formal transfer policies, procedures, and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
* Users follow ABC Company acceptable use policies when transmitting data and take particular care when transmitting or re-transmitting Confidential data received from non-ABC Company Staff.
* Strong cryptography and security protocols (e.g. TLS, IPSEC, SSH, etc.) are used to safeguard sensitive data during transmission over open, public networks. Such controls include: Only trusted keys and certificates are accepted, the protocol in use only supports secure versions or configurations, and the encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include, but are not limited to, the Internet, Wireless technologies, including 802.11 and Bluetooth, cellular technologies (e.g. Global System for Mobile communications (GSM), Code division multiple access (CDMA)), General Packet Radio Service (GPRS), and satellite communications.
* Confidential information transmitted as an e-mail message is encrypted. Any confidential information transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with ABC Company must be encrypted or be transmitted through an encrypted tunnel (VPN) or point-to-point tunnel protocols (PPTP) that include newer versions of transport layer security (TLS).
* Wireless (Wi-Fi) transmissions that are used to access ABC Company portable computing devices or internal networks must be encrypted.
* Encryption is required when users access ABC Company data remotely from a shared network, including connections from a Bluetooth device to a mobile device.
* The secure encrypted transfer of documents and data over the Internet using file transfer programs such as “secured FTP” (FTP over SSH) and secure copy command (SCP).
* All non-console administrative access such as browser/web-based management tools are encrypted using strong cryptography.
* All implementations of SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.

E. Encryption Key Management

Effective key management is the crucial element for ensuring the security of any encryption system. Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with the Electronic Data Retention Policy requirements. ABC Company key management systems are characterized by following security precautions.

ABC Company uses procedural controls to enforce the concepts of least privilege and separation of duties for personnel. These controls apply to persons involved in encryption key management or who have access to security-relevant encryption key facilities and processes, including Certificate Authority (CA) and Registration Authority (RA), and/or contractor personnel. IT security personnel shall verify backup storage for Key passwords, Files, and related backup configuration data to avoid single point of failure and ensure access to encrypted data.

Key management should be fully automated, e.g., IT personnel do not have the opportunity to expose a key or influence the key creation. Keys in storage and transit must be encrypted. Private keys must be kept confidential. Keys must be randomly chosen from the entire key space, using hardware-based randomization.

Key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key, e.g., a key-encrypting-key is used to encrypt other keys, securing them from disclosure.

The resource Owner should be the person responsible for establishing data encryption policies that might include granting exceptions based upon demonstration of a business need and an assessment of the risk of unauthorized access to or loss of the data.

The Chief Security Officer (CSO) shall ensure:

* Decryption keys are not associated with user accounts.
* Documentation and procedures exist to protect keys used to secure stored sensitive data against disclosure and misuse. This requirement applies to keys used to encrypt stored sensitive data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.
* Restricted access to cryptographic keys to the fewest number of custodians necessary.
* Secret and private keys used to encrypt/decrypt sensitive data is stored in one (or more) of the following forms at all times: Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data encrypting key, within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device), as at least two full-length key components or key shares, in accordance with an industry accepted method.
* Cryptographic keys are stored in the fewest possible locations.
* Key management processes and procedures for cryptographic keys are fully documented.
* Cryptographic key changes for keys that have reached the end of their crypto period (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).
* Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.
* If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.
* The generation, use ,and destruction of keys is based on proven processes.
* Cryptographic key custodians formally acknowledge that they understand and accept their key-custodian responsibilities.
* An annual evaluation of encryption algorithms and key sizes used within the organization.

F. Encryption of Data

Users are encouraged to encrypt files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. ABC Company makes available software and procedures approved by the CSO that provide robust encryption, as well as the capability for properly designated ABC Company officials to decrypt the information when required and authorized under this policy. Users encrypting information shall only use the endorsed software and protocols. ABC Company Staff may only encrypt with the permission of his or her supervisor. Data shall only be encrypted using ABC Company approved software and procedures that provide the ability for ABC Company to recover the data. Such endorsed software and procedures shall be updated as technical solutions and ABC Company requirements change.

# V. Enforcement

Any Staff 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 Staff members with access to ABC Company’s Information Resources.

**Policy History**

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

**References:**

COBIT EDM01.01, APO12.02, APO13.07, APO14.01-02, APO14.07, MEA03.01

GDPR Article 25, 32

HIPAA 164.312(a)(2)(iv)

ISO 27001 A.5.1.1, A.10

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 SC-12, SC-13, SC-17

NIST Cybersecurity Framework ID.GV-3, ID.RA-6, ID.RM-1, PR.DS-1-2, DE.DP-2

PCI 2.1.1, 2.3, 3.4.1, 8.2.1, PCI Software Security Framework