End User Encryption Key Protection Policy

1.0 Purpose

Effective encryption relies on the secure management of cryptographic keys. Improper handling, storage, or distribution of encryption keys, particularly private keys or symmetric keys, can lead to their compromise, negating the security provided by encryption and potentially exposing sensitive organizational data. While users may understand the need to encrypt data, specific practices for protecting the keys themselves are crucial. This policy outlines the minimum requirements for securely managing and protecting encryption keys under the control of end users to prevent unauthorized disclosure or fraudulent use.

2.0 Scope

This policy applies to all employees, contractors, consultants, and other personnel ("Users") who generate, possess, manage, or use cryptographic keys for organizational business purposes. It specifically covers the management and protection of:

* Encryption keys issued by or on behalf of the organization.
* Encryption keys used for conducting organizational business.
* Encryption keys used to protect data owned by the organization.

This policy applies to both symmetric (secret) keys and the private keys of asymmetric (public-key) key pairs. Public keys contained within digital certificates are generally considered public information and are exempt from the protection requirements outlined herein (though the integrity of certificates is managed via PKI processes).

3.0 Policy Statements

All encryption keys covered by this policy must be protected diligently against unauthorized disclosure, modification, loss, or misuse.

3.1 General Protection Principles

* The level of protection applied to an encryption key must be at least as strong as the protection required for the data it encrypts.
* Keys must be generated, stored, used, and destroyed using organization-approved methods and tools that adhere to cryptographic best practices.

3.2 Symmetric (Secret) Key Management

*   **Distribution:** When symmetric keys must be distributed, the distribution method must be secure. Keys must be encrypted during transit using a strong, approved asymmetric algorithm (referencing the Acceptable Encryption Policy) or an equally strong symmetric algorithm with a key that meets or exceeds the strength of the key being distributed. If distributing keys for the strongest approved algorithm, techniques like key splitting (encrypting portions with different keys and sending via separate channels) should be employed.
*   **Storage:** Symmetric keys, when stored at rest, must be protected using encryption or access control mechanisms at least as stringent as those used for their secure distribution.

3.3 Asymmetric (Public Key) Private Key Management

Asymmetric cryptography uses public/private key pairs. While the public key is shared, the private key must remain confidential and securely managed by the user.

*   **Organization PKI Keys (e.g., on Smart Cards):**
    *   Private keys associated with the organization's Public Key Infrastructure (PKI), often used for digital signatures and encryption, may be generated and stored on secure hardware tokens like smart cards issued to users.
    *   Private keys used *only* for digital signatures (identity certificates) should ideally be non-exportable and remain solely on the hardware token. Escrow of such signing-only private keys is generally not performed and may be technically infeasible or prohibited.
    *   Private keys used for *data encryption* **must** be securely backed up and escrowed according to organizational procedures managed by the designated IT authority (e.g., Precision Computer Team or Identity Management group). This ensures data recovery if the user's key is lost or unavailable. Refer to the organization's Certificate Practice Statement or related documentation for escrow details.
    *   Access to private keys stored on organization-issued hardware tokens (e.g., smart cards) must be protected by a strong PIN or password known only to the user, compliant with the Password Policy. The device/software must require PIN/password entry for each session or operation involving the private key.
*   **Other Software-Generated Keys:**
    *   If key pairs are generated in software (e.g., by an application or browser) and stored as files, the user is responsible for their protection.
    *   The private key file must be protected with a strong password or passphrase compliant with the Password Policy.
    *   Users **must** create at least one secure backup of software-based private keys used for encryption.
    *   Users **must** provide a copy of any software-based private key used for *data encryption* to the designated organizational authority (e.g., local Information Security representative, IT Help Desk) for secure escrow, following established procedures.
    *   Backup and escrow copies must be protected with strong passwords/passphrases compliant with the Password Policy. Storage of escrowed keys by the organization will adhere to requirements in the Certificate Practice Statement or equivalent documentation.
*   **Commercial / External PKI Keys:**
    *   When interacting with external partners requires using keys from commercial CAs (e.g., VeriSign/DigiCert, Thawte) or partner PKIs, these keys are often generated and stored within

software (e.g., a web browser's certificate store).
    * Users must protect access to these software-based key stores with a strong password. Browser or application settings should be configured to require this password upon accessing the private key. Users remain responsible for securely backing up these keys if used for critical data encryption or access. Escrow requirements may apply if used for encrypting organizational data.
* **PGP Keys:**
    * PGP key pairs may be stored in key ring files on a hard drive or preferably on a hardware token (e.g., secure USB drive, smart card).
    * Access to the PGP private key(s) must be protected by a strong passphrase compliant with the Password Policy.
    * PGP software should be configured to require passphrase entry for each use of the private key.

3.4 Hardware Token Security

* Hardware tokens (smart cards, USB tokens, etc.) storing encryption keys are considered sensitive organizational assets.
* They must be physically secured according to the organization's Physical Security policy, especially when outside organizational premises.
* Tokens must not be left unattended or connected to computers when not actively in use.
* When traveling, tokens should ideally be carried separately from the computer they are used with.

3.5 Authentication (PINs, Passwords, Passphrases)

* All PINs, passwords, or passphrases used to protect encryption keys or access to hardware tokens must meet the complexity, length, and management requirements defined in the organization's Password Policy.

3.6 Loss, Theft, or Compromise Reporting

* The loss, theft, or suspected compromise (unauthorized disclosure or access) of any encryption key covered by this policy, or any hardware token containing such keys, **must be reported immediately** to the designated IT authority (e.g., Precision Computer Team or IT Help Desk).
* IT personnel will guide the user through necessary actions, including key/certificate revocation and replacement procedures.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including audits of key management practices, review of PKI configurations, checks on escrow procedures, user awareness assessments, and investigation of reported incidents.

4.2 Exceptions

Any exception to this policy requires formal, documented justification, risk assessment, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security).

4.3 Enforcement

Failure to comply with this policy, particularly regarding key protection, escrow, or incident reporting, may result in disciplinary action, up to and including termination of employment or contract. It may also lead to revocation of access privileges or certificates.

5.0 Definitions

* **Certificate Authority (CA):** An entity trusted to issue, manage, and revoke digital certificates.
* **Digital Certificate:** An electronic document binding a public key to an identity (user, device, service), signed by a CA.
* **Digital Signature:** A cryptographic mechanism using a private key to sign data, allowing verification of origin and integrity using the corresponding public key.
* **Hardware Token:** A physical device (e.g., smart card, USB key) used to store cryptographic keys securely and potentially perform cryptographic operations.
* **Key Escrow:** The practice of securely storing a copy of a cryptographic key (typically a private encryption key) with a trusted third party or organizational authority to allow for data recovery.
* **PGP (Pretty Good Privacy):** A popular encryption program providing cryptographic privacy and authentication, often used for email and file encryption.
* **PIN (Personal Identification Number):** A short numeric or alphanumeric code used for authentication, often to access a hardware token.
* **Private Key:** The secret component of an asymmetric key pair.
* **Public Key:** The publicly shared component of an asymmetric key pair.
* **Public Key Cryptography (Asymmetric Cryptography):** A cryptographic system using pairs of keys (public and private).
* **Symmetric Cryptography (Secret Key Cryptography):** A cryptographic system using the same key for encryption and decryption.

6.0 Related Policies

* Acceptable Encryption Policy
* Certificate Practice Statement (or equivalent PKI documentation)
* Password Policy
* Physical Security Policy
* Data Classification Policy
* Information Handling Policy

Revision #3
Created 28 August 2024 16:51:42 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery