SecOps® Solution

End User Encryption Key Protection Policy

Free Use Disclaimer: *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new policy or an updated version of this one.*

1. Overview

Inadequate encryption key management can result in the compromise and exposure of the private keys used to protect sensitive data, which compromises the data itself. Users could be aware of the need to encrypt some documents and electronic conversations, but they might not be aware of the minimal security requirements for encryption keys.

2. Purpose

An end-user encryption key protection policy outlines the procedures and guidelines for safeguarding encryption keys used by end users to secure sensitive data. The security measures described include operational and technical safeguards such as key backup procedures, encryption with a different key, and usage of tamper-resistant hardware.

3. Scope

This policy applies to any encryption keys listed below and to the person responsible for any encryption key listed below. The encryption keys covered by this policy are

- encryption keys issued by **<Company Name>**
- encryption keys used for **<Company Name>** business
- encryption keys used to protect data owned by **<Company Name>**

This regulation expressly excludes the public keys present in digital certificates.

4. Policy

All encryption keys covered by this policy must be protected to prevent unauthorized disclosure and subsequent fraudulent use.

4.1 Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in **<Company Name>**'s Acceptable Encryption Policy. If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized, and each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for the distribution of that key.

4.2 Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it is issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

4.2.1 <Company Name>'s Public Key Infrastructure (PKI) Keys

The public-private key pairs used by the 's public key infrastructure (PKI) are generated on the tamper-resistant smart card issued to an individual end user. The private key associated with an end user's identity certificate, which is only used for digital signatures, will never leave the smart card. This prevents the Infosec Team from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed in compliance with policies.

Access to the private keys stored on an issued smart card will be protected by a personal identification number (PIN) known only to the individual to whom the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed.

4.2.2 Other Public Key Encryption Keys

Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the public-private key pair is generated on a smartcard, the requirements for protecting the private keys are the same as those for private keys associated with **<Company Name's>** PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage.

The Infosec Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with **<Company Name>** Password Policy. Infosec representatives will store and protect the escrowed keys as described in the **<Company Name>** Certificate Practice Statement Policy.

4.2.3 Commercial or Outside Organization Public Key Infrastructure (PKI) Keys

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end-user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

4.2.4 PGP Key Pairs

If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's keyring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart card. Since the protection of the private keys is the passphrase on the secret keying, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

4.3 Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in <Company Name>'s Physical Security policy when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. End users traveling with hardware tokens, will not be stored or carried in the same container or bag as any computer.

4.4 Personal Identification Numbers (PINs), Passwords, and Passphrases

All PINs, passwords, or passphrases used to protect encryption keys must meet complexity and length requirements described in <Company Name>'s Password Policy.

4.5 Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to The Infosec Team. Infosec personnel will direct the end user in any actions that will be required regarding the revocation of certificates or public-private key pairs.

5. Policy Compliance

5.1 Compliance Measurement: The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions: The Infosec team must beforehand approve any exception to the policy.

5.3 Non-Compliance: An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies, and Processes

- Password Protection Policy

7. Definition and Terms

None.

8. Revision History

Version	Date	Description
1.0	14-02-2023	Initial Policy