*Encryption and Key Management Policy*

Table of Contents

[Purpose 1](#_Toc3961361)

[Scope 1](#_Toc3961362)

[Policy 1](#_Toc3961363)

[Authorization 1](#_Toc3961364)

[Algorithms 1](#_Toc3961365)

[Requirements 2](#_Toc3961366)

[Review 2](#_Toc3961367)

[Key Management 2](#_Toc3961368)

[Key Generation 3](#_Toc3961369)

[Key Security 4](#_Toc3961370)

[Violations 5](#_Toc3961371)

[Definitions 5](#_Toc3961372)

[References 6](#_Toc3961373)

[Related Documents 6](#_Toc3961374)

[Approval and Ownership 6](#_Toc3961375)

[Revision History 6](#_Toc3961376)

Purpose

This policy defines the requirements for establishing the encryption implementation and management requirements related to the CompanyX (the “Company”) Information systems infrastructure.

Scope

This policy applies to all CompanyX Information systems and facilities, with a target audience of CompanyX Information Technology employees and Third-Parties.

Policy

### ****Authorization****

**Only Approved Encryption Systems** - Encryption tools or processes must not be used for CompanyX information unless they are approved by the Information Security Manager.

### ****Algorithms****

**Standard Encryption Algorithm And Implementation** - If encryption is used, government-approved standard algorithms and standard implementations must be consistently employed.

**Publicly-Evaluated Encryption Algorithms** - Every general purpose encryption algorithm used to protect CompanyX production information and information systems must be open (that is, the specific mechanisms are publicly disclosed) and must have been evaluated by cryptography experts.

### ****Requirements****

**Encryption Process Hardware Modules** - All encryption related processes must be performed in tamper-resistant hardware modules. This approach minimizes the threat of software reverse engineering and unauthorized disclosure of key(s).

**Encryption Keys Not Resident In Main Memory** - Encryption keys must never be resident in main memory, buffers, or registers on the production computers where they are employed for security processes. Instead they must be resident in peripheral hardware devices known as security modules, key loaders, or other dedicated purpose devices.

**User-Chosen Encryption Key Length** - Whenever user-chosen encryption keys are employed, the encryption system must prevent users from employing keys made-up of less than 10 characters.

**Systems Design Encryption Key Length** - CompanyX production system encryption systems employing symmetric algorithms must have a key length of at least 128 bits. Asymmetric algorithms must employ a key length which, in the estimation of the Information Security Department, provides a comparable level of security.

**Encryption And Digital Signature Key Separation** - If both encryption and digital signatures are used, separate keys must be used for each of these two control measures.

**Electronic Messaging Encryption** - All sensitive information including, but not limited to, credit card numbers, passwords, and research and development information must be encrypted when transmitted through any end-user electronic messaging system.

**Disk Encryption - Access Control -** In all instances where disk encryption is used to protect CompanyX information, logical access must be managed independently of native operating system access control mechanisms.

**Encryption System Initialization** - Whenever an encryption system to be used for CompanyX production information systems is being initialized, installed, enabled, or reset, a computer audit specialist must be present. This specialist must observe and document each step of these processes.

### ****Library Review****

**Only Approved Cryptographic Libraries Used in Development** - All in-house or Third-Party developed applications must only use cryptographic controls documented and approved by the Information Security Department.

**Annual Review of Cryptographic Libraries Used in Development** - CompanyX must annually review and approve a list of cryptographic controls used within production applications. The list must be approved by members of both the Information Security and Legal Departments.

### ****Key Management****

**Encryption Key Management Systems** - CompanyX encryption systems must be designed such that no single person has full knowledge of any single encryption key.

**Management Responsibility Delegation** - Key management responsibility must be delegated only to a party who has passed a background check, passed an operational security audit, and signed a confidentiality agreement.

**Data And Encryption Key Transmission** - If encryption is used, and if keys are transmitted to a remote party in a readable form, then the information protected with encryption must be transmitted over a different communication channel than the keys used to govern the encryption process.

**Automated Encryption Key Management** - Whenever such facilities are commercially available, CompanyX must employ automated key management processes, rather than manual key management processes.

**Two Of Four People With Access To Master Keys** - Access to CompanyX production system encryption master keys must be provided only if at least two, of a total of four, trusted and authorized individuals are simultaneously present. Alternatively, these two individuals may be securely represented simultaneously through a computer network.

**At Least Two People With Access To Master Keys** - At all times, at least two trusted and authorized people must have access to the encryption master keys used to protect production information.

**Key Exchange Material Destruction** - Custodians of key exchange material must destroy this material according to approved procedures within a reasonable time, not to exceed 10 business days, following the successful verification of a key exchange process.

**Private Encryption Key Transmission** - If private encryption keys are transmitted over communication lines, they must be encrypted with a stronger algorithm than is used to encrypt other sensitive data protected by encryption.

**Public Key Changes** - If a public encryption key has been posted on a web server or in another publicly accessible location, all regular correspondents with whom this key has been used must be notified whenever there is a change in this public key.

**Compromised Keys** - Encryption keys that have been compromised, or revealed to Third-Parties under a key escrow arrangement, must immediately be revoked retroactively to the last time and date when the keys were known to be safe.

**Key Recovery Operation Controls** - Two authorized CompanyX staff members must be present whenever keys are recovered from an encryption key archive and all such operations must be securely logged.

**Key Management Responsibility** - Whenever encryption is used to protect sensitive data, the relevant Owner of the data must explicitly assign responsibility for encryption key management.

**Unauthorized Key Substitution** - Key management procedures must be implemented to prevent the unauthorized substitution of encryption keys.

**Key Custodian Acknowledgement** - Encryption key custodians must sign a form specifying that they understand and accept their key custodian responsibilities.

### ****Key Generation****

**Encryption Key Life** - Keys used for encrypting CompanyX data must be changed at least every 90 days.

**Encryption Key Expiration** - All encryption keys must have a stated life and must be changed on or before the stated expiration date.

**Encryption Key Generation** - Whenever encryption is used, the keys employed must be generated by means that are not practically discernible by an adversary, and that will yield keys that are difficult-to-guess.

**Key Generation Materials** - Whenever encryption is used, materials to develop encryption keys and hardcopy versions of keys must be kept locked-up when not in use. Protective measures to prevent these keying materials from falling into the wrong hands must be observed throughout the life cycle of the information protected by the keys.

**Key Generation Material Destruction** - All supplies used for the generation, distribution, and storage of keys (such as carbon copies, printer ribbons, and the like) must be protected from disclosure to unauthorized persons. When they are no longer needed, they must be destroyed by pulping, shredding, burning, or other approved methods.

**Encryption Key Change Interval** - Keys used for encrypting CompanyX data must be changed at least once every year.

### ****Key Security****

**Encryption Key Disclosure — Approval** - Encryption keys are a most sensitive type of information, and access to such keys must be strictly limited to those who have a need-to-know. Unless the approval of a Senior Vice President is obtained, encryption keys must not be revealed to consultants, contractors, or other Third-Parties.

**Encryption And Digital Signature Key Storage** - Keys employed by end users for encryption and digital signatures must always be stored in a tamper-resistant hardware device, such as a smart card.

**Backup Encryption Keys** - If a CompanyX worker is going to employ encryption for production business information processing activities, the worker must securely deposit backup copies of all keys with the Information Security Department.

**General Purpose Encryption Systems** - All general-purpose encryption processes running on CompanyX information systems must include key escrow functions. These special functions allow CompanyX management to recover encrypted information should there be system errors, human errors, or other problems.

**Encryption Key Secrecy** - The secrecy of any encryption key used for confidentiality purposes (e.g., for data encryption or as a seed to an access control system) must be maintained until all of the protected information is no longer considered confidential.

**Plaintext Encryption Master Keys** - Only two approaches for protecting plaintext (readable) master keys are acceptable to CompanyX. Master keys may be manually handled via dual control with split knowledge. Alternatively, they may be stored in tamper-proof modules. In all other places, they must appear only in encrypted form.

**Encryption Key Storage Media** - If encryption is used to protect sensitive data resident on computer storage media, the encryption keys and related encryption keying materials used in the encryption process must not be stored anywhere on this storage media in unencrypted form.

**Encryption Key Duplication** - Encryption keys used to conceal backup data must themselves be backed-up and must be stored with security measures comparable to or more stringent than measures applied to the involved backed-up data.

**Encryption Key Disclosure — Controls** - Encryption keys must be protected from unauthorized disclosure through technical controls such as encryption under a separate key and use of tamper-resistant hardware.

**Digital Certificate Private Key Security** - The private key associated with each worker at CompanyX must be protected against unauthorized disclosure when not in use by utilizing techniques beyond physical security.

**Digital Signature And User Authentication Keys** - Keys used for digital signatures, digital certificates, and user authentication must never be included in a key escrow arrangement.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. CompanyX reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. CompanyX does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, CompanyX reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

Any employee or Third-Party who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

**Algorithm** - The mathematical operation used for the encryption of information.

**Digital Certificate** - An attachment to an electronic message used for to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

**Digital Signature** - An electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

**Encryption** - The conversion of data into a form that cannot be easily understood by unauthorized people.

**Encryption Key** - A string of characters that is unique to an entity that when used in conjunction with a cryptographic algorithm determines the specific operation of that algorithm to render the original information unreadable.

**Encryption Key Escrow** - The processes of managing, e.g., generating, storing, transferring, auditing, the two components of an encryption key by two key component holders.

**Private Encryption Key** - Input to public key cryptographic algorithm that is uniquely associated with an entity and is not made public, used to encrypt information.

**Public Encryption Key** -Input to a public key cryptographic algorithm, uniquely associated with an entity and mathematically linked with a corresponding private key, used to encrypt information.

**Third-Party** - Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

References

ISO/IEC 27002: 10. Cryptography

NIST: SC-12 Cryptographic Key Establishment and Management

PCI-DSS: 3.5 Cryptographic Key Management

US-CSF: PR.DS-5: Protections against data leaks are implemented

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |