Cryptographic Erasure System Certification for Cloud
CE-C Certification Criteria Guidelines
Version 1.0

Introduction

Consistent with the Information system Security Management and Assessment Program (ISMAP), the "Guidelines for Information Security Policies in Local Governments" issued by the Ministry of Internal Affairs and Communications require that data stored on virtual servers (logical volumes) hosted on cloud services be erased through cryptographic erasure.

To achieve cryptographic erasure, organizations shall be able to confirm and demonstrate that the target logical data and the associated cryptographic keys are managed appropriately.

With regard to technical confirmation and verification, demonstration trials conducted prior to the establishment of this certification scheme confirmed the effectiveness of log management.

However, these trials also identified a number of issues in the encryption and key management processes needed to achieve cryptographic erasure. Resolving these issues required a study conducted jointly with the relevant parties.

Accordingly, the Cloud Service Provider Certification Standards Working Group was established in March 2023 to define the following business process for the encryption and key management operations required to implement cryptographic erasure.

• Standardizing the operational system for data encryption on cloud virtualization servers
• Standardizing the cryptographic key management method and operational system that is used when configuring data encryption
• Developing a checklist for the cryptographic key management process based on the above

Please note that some provisions of this guideline may relate to patent rights, patent applications published after filing, or utility model rights.
Neither the Minister of Internal Affairs and Communications nor the Cloud Service Provider Certification Standards Working Group is responsible for identifying or confirming any such patent rights, published patent applications or utility model rights.

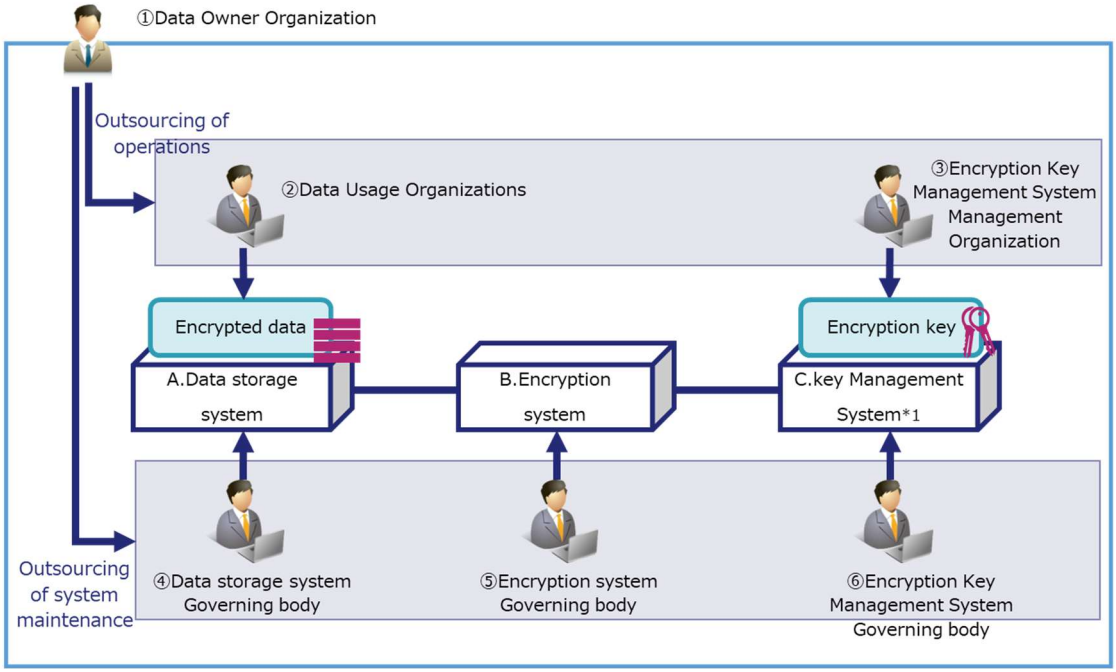
Table of Contents

Roles of the Actors

When considering cryptographic erasure, the roles of each actor — the Data Owner, the Data Storage System, the Encryption System, and the Key Management System — shall be taken into account.

The following diagram illustrates the definition and role of each actor.

The Role of Actors



*1）The key management system shall be limited to enclosures or virtual appliances that have been certified to FIPS140-2, and shall not include the surrounding environment.

- **Data Owner Organization:**
  The organization that holds ownership of the data.
  Take full responsibility for the handling of its own data.
  May transfer part of that responsibility to a service provider through the use of external services.
- **Data User Organization:**
  Responsible for the managing data, input, output, and reference of data.
  Actual operational personnel.
- **Key Management System Management Organization:**
  Responsible for the management of cryptographic keys, including generation and destruction.
- **Data Storage System Management Organization:**
  The organization that manages the Data Storage System.
  Provide a secure data storage environment.
- **Encryption System Management Organization:**
  The organization that manages the Encryption System.
  Provides encryption using a secure encryption method.
- **Encryption Key Management System Management Organization:**
  The organization that manages the Key Management Systems.
  Provides key management functions that enables cryptographic erasure.

Definitions of the System in the Cryptographic Erasure Cloud Service Provider Certification Criteria

1.Data storage system: a system in which encrypted data is stored.

2. Encryption system: a system that performs encryption processing before data is written to non-volatile media in a Data Storage System.

3.Key management system: a system that manages the keys used for encryption and decryption by an Encryption System.

A. Data Owner

Assessment Requirements

A. Data Owner

A.1. Information Security Policy

A.1.1.

The Key Management System management organization shall establish an information security policy to protect data. The information security policy shall state the following:

a) It is appropriate to the purpose of the organization;

b) It includes information security objectives or provide a framework for setting information security objectives;

c) It includes a commitment to satisfy applicable requirements related to information security;

d) The Access control policy for key information and encrypted data

Guidance

An information security policy expresses the Data Owner organization's top management commitment regarding encryption and erasure, both internally and externally. Accordingly, the information security policy should be formulated taking into account items a) through d) above.

Ensuring suitability:
The information security policy should be appropriate to the organization's objectives and consistent with the objectives of the Key Management System.

Clarification of information security objectives:
The information security policy should clearly state the purpose of information security and provide a framework for the Key Management System to protect data and maintain its confidentiality and integrity.

Statement of commitment:
The information security policy should include an organization-wide commitment to satisfying applicable information security requirements. The Organization should commit to providing the resources and support necessary to implement and comply with the policy.

Defining access control policy:
The information security policy should clearly define the access control policy for key information and encrypted data. The access control policies should include authentication, authorization, and auditing processes, and should establish appropriate procedures to maintain confidentiality.

Change management and auditing:
The information security policies define change management processes and provide mechanisms for addressing changing security requirements and new threats. The policy should be audited and reviewed periodically to confirm that it is being implemented effectively and appropriately.

Education and awareness:
The information security policy should provide resources and programs to educate and raise awareness among interested parties, both inside and outside the organization. All interested parties should understand and comply with the policy and appropriate training and information should be provided to support this.

A.2. System configuration, and Organizational Structure, roles

A.2.1.

The Data Owner organization shall prepare documented information that can confirm the roles, responsibilities, and organizational structure of its own personnel who perform work related and system configuration related to key information and encrypted data, or of any other organization to which such work

Guidance

The system configuration, structure, and role should clarify the organizational structure and the roles of the Data Owner in relation to cryptographic erasure.
This should be clarified in regulations, organization charts, and similar documents, taking into account the following items.

Clarification of roles and responsibilities:
The Data owner organizations shall clearly define the roles and responsibilities of their own personnel who perform work related to key information and encrypted data, as well as

those of external organizations to which such activities are delegated. It is recommended that documented information be maintained, including the duties, scope of responsibilities, and contact information of each individual or organization.

Organizational structure:
The Data Owner organization shall establish an appropriate organizational structure for performing work and system configuration related to key information and encrypted data. This structure should include the necessary resources, authority, oversight, and contact information.

Creating documented information:
The organization should create documented information that confirms the roles, responsibilities, and structure related to work related to key information and encrypted data and system configuration. Such Documented information should be clear, contain specific detail, and be stored in a location that is easily accessible to interested parties.

Regular reviews and updates:
Documented information should be reviewed regularly and updated as necessary. When changes occur to the contents of documented information such as when changes are made or new personnel are added, documented information should be updated promptly.

Notification and Education of Interested parties:
Documented information concerning work and systems related to key information and encrypted data should be appropriately communicated and explained to interested parties. Necessary education and training should be provided so that those involved understand their roles and responsibilities and can perform their duties appropriately.

A.2. System configuration, structure, roles
A.2.2.
The Data Owner organization shall prepare documented information that confirms the configuration and data flow of the system that handles key information and encrypted data.

Guidance

The Data Owner organization shall prepare documented information that confirms the configuration and data flow of the system that handles key information and encrypted data. This documented information should be clarified using a configuration diagram of the system concerned. From this perspective, the configuration and data flow of the system handling key information and encrypted data should be documented, taking into account the following items.

Clarification of system configuration:

The Data Owner organization shall clearly document the configuration of system that handles key information and encrypted data. This documented information should preferably include the system's hardware, software, and network configuration, etc.

Data flow description:

The data flow relating to the handling of key information and encrypted data should be described. The procedures and processes from the point of data generation through storage, processing, transfer, and deletion should be clearly described.

Description of security measures:

Documented information should describe the security measures related to the system configuration and data flow. Specific measures to strengthen security — such as access control, encryption, and audit logging settings — should be included.

Description of integration and dependencies between systems:

The organization should clearly explain how the system that handles key information and encrypted data is integrated with other systems and identify any dependencies. How data is exchanged and shared with other systems should be described.

Documented information updates and reviews:

Documented information should be reviewed periodically and updated as necessary. It should be updated appropriately whenever the system is changed or upgraded, or when new security requirements are introduced.

Sharing and educating interested parties:

Documented information related to system configuration and data flow should be appropriately shared with, and understood by, interested parties. Appropriate education and training should be provided so that interested parties understand the system configuration and data flow, and recognize their importance to security.

A.2. System configuration, structure, roles

A.2.3.

The Data Owner organization shall prepare documented information that enables the managing organization to be confirmed for each of the following systems that handle key information and encrypted data.

- **Data Storage System management organization**
- **Encryption System management organization**
- **Key Management System management organization**

Guidance

The Data Owner organization should prepare documented information that enables the managing organization to be confirmed for the Data Storage System management organization, the Encryption System, and the Key Management System management organization that handle key information and encrypted data. This should be clarified using relevant regulations, configuration diagrams, and similar documents. From this perspective, documented information should confirm the management organization for each system, taking into account the following items.

Creating documented information:

Data owner organizations shall create management documented information for each system that handles key information and encrypted data. This preferably includes information regarding the Data Storage System management organization, Encryption System, and Key Management System management organization.

Clarification of roles and responsibilities of each system:

The documented information should clearly state the roles and responsibilities of each system, including the role of the Data Storage System management organization, the functions of the Encryption System, and the responsibilities of the Key Management System management organization.

System configuration and data flow description:
Information regarding the configuration and data flow of each system shall be described in detail, clearly indicating the data flow, processing procedures, storage locations, and interactions between systems.

Verifying security measures and regulatory compliance:
The documented information should clearly state the security measures adopted by each system and the regulations with which it must comply, including specific details of access controls, encryption algorithms, and audit requirements.

Regular updates and reviews of documented information:
Documented information should be reviewed periodically and updated as necessary, and kept up to date to address system changes and emerging security threats.

Sharing and educating interested parties:
Documented information should be appropriately shared with, and understood by, interested parties. Appropriate education and training should be provided so that interested parties understand the role and security importance of each system.

A.3. Management Responsibilities

A.3.1.

The management of the Data Owner organization shall establish a system to appropriately communicate key points regarding information security roles and responsibilities to its own personnel who perform work related to key information and encrypted data and system configuration, or to other organizations to whom such work is outsourced.

Guidance

The management of the Data Owner organization should establish a system to appropriately communicate key points regarding information security roles and responsibilities to its own personnel who perform work related to key information and encrypted data and system configuration, or to other organizations to whom such work is outsourced. Possible ways to prepare this information include creating a role/responsibility

table. When developing these roles and responsibilities. The following items should be considered when establishing this mechanism:

Clarification of roles and responsibilities:
The management of Data Owner organization shall clearly communicate information security roles and responsibilities to personnel who work on key information and encrypted data, and to other organizations to which work is outsourced. This should include specific points for understanding the roles and responsibilities of each personnel, as well as the importance of security.

Education and awareness programs:
Management of the Data Owner organization should develop an education and awareness program regarding information security roles and responsibilities. This should include regular security training, security awareness campaigns, and training based on specific scenarios.

Establishing means of communication:
Communication channels should be established to appropriately convey the key points regarding information security roles and responsibilities. These may include meetings, workshops, email, and internal portals.

Confirmation prior to granting access:
A process should be established to confirm that the key points regarding information security roles and responsibilities have been understood before access is permitted. The granting of access rights or privileges should be based on appropriate training and awareness-confirmation procedures.

Emphasis on compliance:
When conveying the key points regarding information security roles and responsibilities, management of the Data Owner organization should emphasize the importance of compliance. It should be clearly communicated that following appropriate procedures and policies is essential to ensuring organization security and trustworthiness.

A.3. Management **Responsibilities**
A.3.2.
The management of the Data Owner organization shall establish a mechanism to provide its own personnel who perform work and system configuration related to key information and encrypted data with guidelines to state what is expected of them regarding information security in their roles within the organization.

Guidance

The management of the Data Owner organization shall establish a mechanism to provide its own personnel who perform work and system configuration related to key information and encrypted data with guidelines to state what is expected of them regarding information security in their role within the organization.

This may be achieved, for example, through management policies communicated by the Data Owner organization's management to personnel. The following items should be considered when establishing this mechanism.

Clarification of expected behavior and responsibilities:

Management of Data Owner organization shall clearly indicate the expected behavior and responsibilities regarding information security to their own personnel who work on key information and encrypted data. This should include adhering to security policies and regulations, best practices, and maintaining confidentiality and data integrity.

Description of roles and responsibilities:

The roles and responsibilities of each worker shall be clearly defined, and the expected role from an information security perspective shall be clearly defined. Guidance should be provided so that personnel understand their responsibilities and can act accordingly.

Risk management and countermeasure proposals:

Management of the Data Owner organization should communicate expectations regarding the recognition and management of information security risks. Appropriate countermeasures and security improvement proposals should be presented to personnel.

Communication and education:

Information security guidelines shall be communicated to personnel through appropriate communication methods. Appropriate education and training should be provided to help personnel understand and implement information security guidelines.

Feedback and improvement process:

Management of the Data Owner organization shall accept feedback on information security guidelines and expectations and establish appropriate improvement processes. A mechanism should be put in place to use feedback from personnel to improve the guidelines and processes.

A.3. Management Responsibilities

A.3.3.

The management of the Data Owner organization shall establish a mechanism to motivate its own personnel who perform work related to key information and encrypted data and system configuration to fulfill with the organization's information security policies.

Guidance

The management of the Data Owner organization shall establish a mechanism to motivate its own personnel who perform work related to key information and encrypted data and system configuration to fulfill with the organization's information security policy. The following items should be considered when establishing this mechanism.

Clear communication of policy:
The management of the Data Owner organization shall clearly define the organization's information security policies and communicate them to personnel. Policies should be concise, easy to understand, and presented in a format that personnel can readily grasp.

Emphasizing the importance of policy:
The importance of information security policies should be emphasized to personnel to foster a culture of security within the organization. Awareness of risks such as data breaches and cyberattacks should be promoted to help personnel understand why the policies matter.

Introducing motivation and reward systems:
Appropriate reward systems and incentives should be introduced to motivate personnel to comply with information security policies. Rewards, recognition, and advancement opportunities for good security practices should be provided to encourage adherence to the policy.

Providing education and training:
Provide education and training to personnel regarding information security policy. Ongoing training programs should be implemented to support understanding and implementation of the policy.

Monitoring and evaluating compliance:
A mechanism should be introduced to monitor and evaluate compliance with the policy. Real-time monitoring and periodic evaluation should be used to confirm that personnel are properly complying with the organization's information security policy.

Feedback and improvement process:
Feedback from personnel should be accepted to promote improvement of policy and processes. Improving security policies in this way should help increase personnel motivation and commitment to security.

A.3. Managemen**t Responsibilities**

A.3.4.

The management of Data Owner organizations shall establish a mechanism to ensure that its own personnel who perform work related to key information and encrypted data and system configuration achieve a certain level of awareness of information security related to their roles and responsibilities within the organization.

Guidance

The management of the Data Owner organization shall establish a mechanism to ensure that its own personnel who perform work related to key information and encrypted data and system configuration achieve a certain level of awareness of information security related to their roles and responsibilities within the organization. The following items should be considered when establishing this mechanism.

Clarification of roles and responsibilities:
Management of the Data Owner organizations shall clearly understand how its own roles and responsibilities affect information security. Roles and responsibilities should be defined, and the extent of involvement in information security made explicit.

Information security training and education:
Management shall participate in information security training and education programs to acquire appropriate knowledge and skills. Opportunities should be provided to deepen understanding of the importance and best practices of information security.

Formulation and compliance of information security policy:
Management shall be actively involved in the formulation and compliance of information security policies, making decisions related to information security in accordance with the policy and overseeing compliance with it.

Leadership and model influence:
Management should demonstrate leadership regarding information security and role-model behavior within the organization. Such role-model behaviors should demonstrate to personnel the importance of information security and help shape the culture of the entire organization.

Emphasizing commitment to information security:
Management should emphasize its commitment to information security and periodically affirm its importance within the organization. This commitment should be demonstrated through regular reporting on information security issues and achievements.

Evaluation and improvement process:
Management should establish a process to evaluate and improve its own level of information security awareness. Feedback should be accepted with the aim of both personnel growth and improving the organization’s security overall capabilities.

A.3. Management **Responsibilities**

A.3.5.

The Data Owner organization's management should put in place a system to ensure that its own personnel who work with key information and encrypted data and configure system configuration comply with the terms of employment, including the organization's information security policy and appropriate work practices.

Guidance

The Data Owner organization's management should put in place a system to ensure that the organization's personnel who perform work related to key information and encrypted data and system configuration comply with the terms of employment, including the

organization's information security policy and appropriate work practices. The following items should be considered when establishing this mechanism.

Communication of information security policy:
Management of the Data Owner organization should clearly communicate the information security policy to personnel and ensure that it is understood. Policies should be presented as part of the terms of employment and personnel should be required to follow them.

Appropriate training and education:
Personnel shall be provided with appropriate training and education regarding information security. Specific guidance and practical training should be given so that personnel acquire the necessary information security skills to comply with the policy.

Clarification of employment conditions:
Employment conditions shall clearly state the information security policy and compliance. Personnel should agree to the information security policy through their employment contract or organizational rules, and compliance should be a condition of employment.

Monitoring and evaluation:
The organization shall regularly monitor and evaluate worker compliance with the information security policy. Monitoring measures and evaluation processes should be in place to ensure compliance with appropriate policies.

Feedback and improvements:
Feedback from personnel should be accepted, and improvements to the information security policy and appropriate methods of working should be implemented. The organization should establish a mechanism to address personnel's questions regarding the policy and to improve the policy accordingly.

Linkage of reward and evaluation:
Personnel compensation and evaluation should consider compliance with the information security policy and contribution to appropriate methods of working. An evaluation system should be established so that appropriate information security efforts are reflected in compensation and promotion decisions.

A.3. Management Responsibilities

A.3.6.

The management of the Data Owner organization shall maintain appropriate skills and qualifications for its own personnel who perform work related to key information and encrypted data and system configuration and establish a system to ensure that they receive regular training.

Guidance

The management of the Data Owner organization shall establish a system in which the organization's personnel who perform work related to key information and encrypted data and system configuration shall maintain appropriate skills and qualifications and receive regular training. The following items should be considered when establishing this mechanism.

Clarification of skill and qualification requirements:
Management of Data Owner organizations should require that personnel who work with key information and encrypted data have appropriate skills and qualifications. The necessary skills and qualifications should be clearly defined, and personnel should be required to maintain them.

Providing of regular educational programs:
Management should provide regular education programs to personnel, providing opportunities to learn the latest information security trends and best practices.
Education programs should cover a comprehensive range of content, from basic information security knowledge to advanced skills, to help improve personnel capability.

Compliance with industry standards and regulations:
Management shall provide educational programs to ensure compliance with information security requirements based on industry standards and regulations. Regular training should be provided to keep personnel up to date with the latest regulations and regulatory changes in the industry.

Encouraging skill improvement:

Management should encourage personnel to improve their skills and promote learning and growth. Rewards and promotion opportunities for outstanding achievements or skill improvement should be provided to help increase personnel motivation.

Regular skills assessment and feedback:
Management should regularly assess personnel skill levels and provide feedback. Feedback should preferably serve as a guide for personnel to self-evaluate and improve.

A.3. Management Responsibilities
A.3.7.
The management of the Data Owner organization shall regularly provide education and competency regarding security and cryptographic keys to its own personnel who work on key information and encrypted data and set up systems.

Guidance
The management of the Data Owner organization shall regularly provide education and competency regarding security and cryptographic keys to its own personnel who work on key information and encrypted data and configure system configuration. The following items should be considered when establishing this mechanism.

Implementation of regular security education programs:
Management of Data Owner organizations should conduct regular training programs on security topics for personnel. Educational programs should provide knowledge about basic principles of information security, security policies, and the latest threats and attack techniques.

Education and training regarding cryptographic keys:
Personnel shall be provided with education and training regarding the generation, management, exchange, and storage of cryptographic keys. Specific guidance should be provided to deepen understanding of the importance of cryptographic keys and how to handle them appropriately.

Periodic evaluation of security practices:

Management should regularly evaluate the security practices of personnel and provide feedback for improvement. Assessment should be conducted through actual work or simulations to help improve personnel's security skills.

Education on the latest security trends:
Personnel should be provided with education on the latest security trends and threats. Knowledge of new threats and attack techniques should be updated regularly to ensure that personnel always have access to the latest information.

Continued emphasis on policies and procedures:
Management should regularly emphasize the importance of security policies and procedures and encourage personnel to comply with them. Policies and procedures should be reviewed regularly to ensure that personnel maintain ongoing compliance.

A.3. Management Responsibilities

A.3.8

Management of Data Owner organizations should establish mechanisms to provide anonymous reporting channels (e.g., whistleblowing) for its own personnel who work with key information, encrypted data, and configure systems to report violations of information security policies or procedures.

Guidance

The management of the Data Owner organization shall establish a mechanism to provide anonymous reporting channels, such as whistleblowing, for reporting violations of information security policies or procedures to the organization's personnel who work on key information and encrypted data and configure system configuration. The following items should be considered when establishing this mechanism.

Clarification of purpose:
The main purpose of establishing an anonymous reporting channel should be clearly defined, and a policy should be formulated to achieve that purpose.

Compliance with legal requirements:
When building an anonymous reporting mechanism, applicable legal requirements and regulations should be confirmed and followed. Particular emphasis should be placed on

confirming and complying with applicable requirements such as personal information protection laws.

Clarification of reporting process:
Clearly define the process for anonymous reporting. All aspects of the process should be clearly specified, including how the reporter will make the report, how anonymity will be maintained, and who will receive the report.

Selection of reporting party:
A person or department within the organization to receive anonymous reports should be designated. The recipient should be a highly reliable person or department that can be expected to handle information appropriately and take suitable action.

Protection of reporters:
Take steps to protect the privacy and safety of anonymous reporters. This should include the introduction of technological measures to prevent the identity of reporters and the provision of legal protection to prevent unfair treatment of reporters.

Verification and response to reports:
Establish a process to review reports received and take appropriate action based on their content. It is advisable to take prompt and appropriate action depending on the severity and urgency of the reported problem.

Transparency and reporter feedback:
Ensuring transparency in the anonymous reporting process and providing appropriate feedback to reporters to encourage them to continue reporting issues with confidence. Information on report results and countermeasures should be shared appropriately within the organization.

Regular evaluation and improvement:
The anonymous reporting process should be evaluated periodically and improved as necessary. The resolution of reported issues and the effectiveness of the process should be evaluated to identify areas for improvement and support continuous security enhancement.

A.3. Management Responsibilities

A.3.9.

Management of the Data Owner organization should demonstrate support for and lead by example for information security policies, procedures and controls.

Guidance

The Data Owner organization's management shall demonstrate support for and lead by example for information security policies, procedures, and controls. The following items should be considered when establishing this mechanism.

Understanding and supporting policies and procedures:
Management should fully understand information security policies and procedures and express clear support for them. This should include increasing your own understanding of information security through participation in training and education programs.

Practicing exemplary behavior:
Management should practice information security best practices themselves and set an example for other employees. This should preferably include proper management of passwords, appropriate handling of confidential information, and compliance with security policies.

Leadership and communication:
Management should demonstrate leadership regarding information security and constantly emphasize its importance to employees. Regular communication and meetings should be used to promote information security initiatives and share related success stories and key points

Risk management and prioritization:
Management shall understand information security risks and prioritize them appropriately. The importance of information security should be considered in resource allocation and investment decisions, and appropriate measures should be required.

Transparency and accountability:
Management shall ensure transparency regarding information security and promise to fulfill its responsibilities to related parties. In the event of an information leak or security incident,

when an information leak or security incident occurs, it should be addressed promptly, and the results and lessons learned should be shared fairly and transparently.

Continuous improvement and learning:
Management demonstrates a commitment to continuous improvement of information security processes and practices and to continuous learning to improve the organization's security capabilities. It should stay informed about the latest trends and best practices in the industry and consider applying them to your organization.

A.4. Contractor management

A.4.1.

The management of the Data Owner organization shall confirm in the policy set, procedures, and controls for information security that another organization to which work related to key information and encrypted data and system configuration is outsourced has the following in place for workers.

- **Mechanism to provide guidelines for demonstrating information security expectations in roles within the organization**
- **Mechanism to motivate the organization to follow a set of policies for information security**
- **Mechanism to achieve a certain level of awareness of information security related to one's role and responsibility within the organization**
- **Mechanisms to ensure compliance with terms and conditions of employment, including the organization's information security policy and appropriate work practices**

Guidance

The management of the Data Owner organization should establish a system for other organizations to which work related to key information and encrypted data and system configuration are outsourced to provide guidelines to personnel to demonstrate their expectations regarding information security. The following items should be considered when establishing this mechanism.

Providing guidance:

Ensure that the other organization provides guidance to personnel setting out their roles and expectations regarding information security. This should ensure that personnel understand their roles and are expected to adhere to appropriate security practices.

Motivation mechanism:
Confirm that a mechanism is in place to motivate other organizations and personnel to comply with information security policies. Ideally, this will include incentive systems, educational programs, and appropriate feedback mechanisms.

Raising awareness:
It should be confirmed that other organizations provide a mechanism to raise its personnel's awareness of information security. This should include training and education programs, evaluation and certification schemes, etc.

Compliance with employment conditions:
Ensure that other organizations and personnel have conditions of employment that ensure that they follow information security policies and appropriate work procedures. This should include contracts, rules, internal regulations, etc.

Education and qualifications provided:
Ensure that other organizations and personnel have appropriate skills and qualifications and provide a mechanism for regular information security training. This encourages personnel to stay informed about the latest security practices and technologies.

Providing anonymous reporting channels:
Verify that another organization provides an anonymous reporting channel for reporting violations of information security policies and procedures. This should make it easier for personnel to report security concerns and issues anonymously.

B. Data Storage System

B. Data Storage System

B.1.Information Security Policy

B.1.1.

The Key Management System management organization shall establish the information security policy to protect data. The following shall be clearly stated in the information security policy.

a) It is appropriate for the purpose of the organization.

b) It includes information security objectives or provide a framework for setting information security objectives;

c) It includes a commitment to meeting applicable requirements related to information security;

d) The access control policy for key information and encrypted data

Guidance

A security policy is an expression of the top-level concept of encryption and deletion as a Data Storage System to the outside and inside of the organization. From this perspective, Accordingly, the information security policy should be formulated taking the following into account.

Ensuring suitability:

Security policies should be appropriate to the organization's objectives and consistent with the objectives of the Key Management System.

Clarification of information security objectives:

The information security policy should clearly state the purpose of information security and provide a framework for the Key Management System to protect data and ensure confidentiality and integrity.

Statement of commitment:

The security policy includes an organization-wide commitment to meeting applicable requirements related to information security. Organizations should commit to providing the resources and support necessary to implement and comply with security policies.

Defining access control policy:

The information security policy should clearly define access control policies for key information and encrypted data. Access control policies should include authentication, authorization, and auditing processes, and provide appropriate procedures to maintain confidentiality.

Change management and auditing:
The information security policies define change management processes and provide mechanisms for addressing changing security requirements and new threats. Audits and evaluations of policies should be conducted on a regular basis to ensure that policies are being effectively and appropriately implemented.

Education and awareness:
The information security policies provide resources and programs to educate and educate interested parties both inside and outside the organization. All interested parties should understand and comply with the policy, and appropriate training and information should be provided to support this.

B.2. System configuration, and Organizational Structure, roles
B.2.1.
The Data Storage System management organization shall prepare documented information that confirms the roles, responsibilities, and organizational structure of the organization's own workers who perform work related to key information and encrypted data and system configuration, or of another organization to which the work is outsourced.

Guidance
System configuration, structure, and role: As a Data Storage System management organization, we clarify the system structure, structure, and role in cryptographic erasure. The system configuration, structure, and roles should be clearly defined in various regulations, organizational charts, etc. From this perspective, it should clarify the system configuration, structure, and roles by considering the following factors.

Clarification of roles and responsibilities:
The Data Storage System management organization shall clearly define the roles and responsibilities of its own personnel who perform work related to key information and

encrypted data, as well as the roles and responsibilities of other organizations to which work is outsourced. This information should be documented, including the scope of work, scope of responsibility, and contact details, for individual or organization.

System development:
The Data Storage System management organization will develop an appropriate system for operations and system configuration related to key information and encrypted data. The structure should include necessary resources, authority, oversight, contact information, etc.

Creating documented information:
Create documented information that confirms the roles, responsibilities, and structure related to work related to key information and encrypted data and system configuration. Documented information should be easy to understand, contain specific information, and be stored in a location that is easily accessible to interested parties.

Regular reviews and updates:
Documented information should be reviewed regularly and updated as necessary. When changes occur to the contents of documented information such as when changes are made or new personnel are added, the documented information should be updated promptly.

Notification and Education of Interested parties:
Appropriately notify and explain documented information regarding work and systems related to key information and encrypted data to related parties. The necessary education and training should be provided so that those involved understand their roles and responsibilities and can carry out their duties appropriately.

B.2. System configuration, structure, roles
B.2.2.
The Data Storage System management organization shall prepare documented information that can confirm the configuration and data flow of the system that handles key information and encrypted data, and its surrounding environment.

Guidance
The Data Storage System management organization shall prepare documented information that confirms the configuration and data flow of the system handles key information and

encrypted data. This should be clarified using a configuration diagram of the relevant system. From this perspective, the configuration and data flow of the system handling key information and encrypted data should be documented, taking into account the following items.

Clarification of system configuration:
The Data Storage System management organization clearly documented information the configuration of the system that handles key information and encrypted data. This documented information should preferably include the system's hardware, software, network configuration, etc.

Data flow description:
The data flow relating to the handling of key information and encrypted data should be described. The procedures and processes from the point of data generation through storage, processing, transfer, and deletion should be clearly described.

Description of security measures:
Documented information should include security measures related to the system configuration and data flow.
Specific measures to strengthen security - such as access control, encryption, and audit logging settings - should be included.

Description of integration and dependencies between systems:
Clearly explain how the system that handles key information and encrypted data is integrated with other systems, and whether any dependencies exist. How data is exchanged and shared with other systems should be described.

Documented information updates and reviews:
Documented information should be reviewed regularly and updated as necessary. It should be updated appropriately whenever the system is changed or upgraded, or when new security requirements are introduced.

Sharing and educating interested parties:

Documented information related to system configuration and data flow should be appropriately shared with and understood by interested parties. Appropriate education and training should be provided so that interested parties understand the system configuration and data flow and understand the importance of security.

B.3. Management Responsibilities

B.3.1.

Management of the Data Storage System management organization should establish a system to appropriately communicate the key points of information security roles and responsibilities to personnel before they are allowed to work on key information, encrypted data, or access system configuration.

Guidance

Management of the Data Storage System management organization should establish a system to appropriately communicate the key points of information security roles and responsibilities to personnel before they are allowed to work on key information, encrypted data, or access system configuration. Possible ways to prepare this information include creating a role/responsibility table. When developing these roles and responsibilities, the following items should be considered.

Clarification of management roles and responsibilities:
Management shall understand the importance of information security and recognize its own responsibility. This should include responsibility for formulating and maintaining information security policiy.

Education and training for personnel:
Personnel should be regularly educated and trained on the importance and responsibility of information security and should be provided with guidelines on how to handle key information and encrypted data and on access privileges to the system.

Dissemination of information security policy:
Disseminate the information security policy within the organization and ensure that all personnel understand and comply with it. Any updates or changes to the policy should be appropriately communicated, and understanding should be confirmed.

Enhanced access control:
Access to key information and encrypted data should be restricted to the minimum necessary privileges. Personnel granted access should be required to operate strictly within the scope of that access.

Audit and evaluation:
The status of information security implementation should be audited periodically and compliance should be evaluated. Areas for improvement should be identified based on the audit results, and appropriate measures should be taken.

Risk management and response:
The Information security related risks should be assessed and appropriate controls formulated. When a security incident occurs, it should be addressed promptly and appropriate measures taken.

Continuous improvement:
Information security policy and procedures should be continually improved to address the latest threats and best practices. A culture in which all members of the organization contribute to improving information security should be fostered.

B.3. Management Responsibilities
B.3.2.
Management of the Data Storage System management organization should establish a system to provide guidelines to workers to indicate information security expectations in their roles within the organization.

Guidance
Management of the Data Storage System management organization should establish a system to provide guidelines to personnel to indicate information security expectations in their roles within the organization. The following items should be considered when establishing this mechanism.

Management leadership:
Management should understand the importance of information security and demonstrate leadership by demonstrating its importance to employees. Organization-wide policies and

objectives for information security should be clearly defined and communicated to employees.

Clarifying information security expectations:
Management should clearly indicate its expectations regarding information security to employees. Personnel should be provided with concrete guidance on data handling, access rights management, and compliance with information security policy.

Providing education and training:
Education and training programs on information security should be conducted regularly within the organization to improve personnel capability. Opportunities should be provided for employees to comply with information security policy and understand security best practices.

Facilitate communication:
Management should communicate important information and changes regarding information security through communication with employees. Employees should be provided with appropriate channels to submit information security concerns and suggestions.

Feedback and improvements:
Management should accept employee feedback and use it to improve information security processes and policies. The effectiveness of information security should be periodically confirmed through continuous monitoring and evaluation, with improvements made as necessary.

Compliance and rewards:
Management should encourage compliance with information security policy and evaluate employees who practice appropriate security measures. A reward system for good information security practices should be introduced to increase employee motivation.

B.3. Management **Responsibilities**
B.3.3.
Management of Data Storage System management organizations shall establish a mechanism to motivate personnel to follow the organization's information security policy.

Guidance

Management of Data Storage System management organizations shall establish a mechanism to motivate personnel to follow the organization's information security policy. The following items should be considered when establishing this mechanism.

Clarification of the organization's information security policy:
Management should clearly define the organization's information security policy and communicate it to employees in an easy-to-understand manner. Policies should include specific policies regarding data storage, access control, security protocols, etc.

Promoting education and awareness:
Educational programs should regularly emphasize the importance of information security to personnel and raise their awareness. Regular training and simulations should be used to inform employees about the latest security threats and countermeasures.

Motivation and rewards:
An incentive system should be introduced to encourage personnel to comply with the information security policy. Rewards for compliance and positive impact of reducing security violations on team or individual evaluation should ne demonstrated.

Feedback and improvements:
Feedback from employees should be accepted, and issues or suggestions concerning policy implementation should be actively incorporated. Identifying areas for improvement or ambiguity and making appropriate modifications should help increase employee satisfaction and compliance.

Role model suggestions:
It is important for executives and managers to take the initiative in complying with information security policies and to set a good role model for employees. Employees should be influenced positively by leadership and be more likely to follow policies.

Continuous monitoring and improvement:
Compliance with the information security policy should be continuously monitored to detect violations or issues at an early stage. The policy should be improved based on monitoring results to raise the organization’s overall security level.

B.3. Management Responsibilities

B.3.4.

The management of a Data Storage System management organization shall establish a system for workers to achieve a certain level of awareness of information security related to their roles and responsibilities within the organization.

Guidance

The management of a Data Storage System management organization shall establish a system for personnel to achieve a certain level of awareness of information security related to their roles and responsibilities within the organization. The following items should be considered when establishing this mechanism.

Clarification of roles and responsibilities:
Management should clearly define its own roles and responsibilities regarding information security and make them clear to personnel, confirming that each individual's role and responsibilities are consistent with information security objectives.

Providing education and training:
Information security education programs and training should be conducted within the organization to improve information security knowledge of both management and personnel. Information security training related to roles and responsibilities should be provided to help achieve the required level of awareness.

Developing regulations and promoting compliance:
Management shall develop information security policy and procedures and promote compliance with them. It is advisable to clearly communicate information Security provisions related to their roles and responsibilities to employees and monitor their compliance.

Audit and evaluation:
The status of information security implementation should be audited periodically, and the level of compliance evaluated. Necessary measures and areas for improvement should be identified based on audit results and addressed appropriately.

Transparency and communication:
Management shall ensure transparency regarding information security and promote communication with personnel. providing appropriate information regarding significant changes or issues related to information security and accepting feedback from employees.

Continuous improvement:
Management shall make continuous efforts to improve information security, and not only maintain a certain level, but also constantly aim for improvement. Information security should be periodically reassessed and improved to respond to new threats and technological advances.

B.3. Management **Responsibilities**
B.3.5.
Management of Data Storage System management organizations should have mechanisms in place to ensure that workers comply with the terms and conditions of employment, including the organization's information security policy and appropriate work practices.

Guidance
Management of Data Storage System management organizations should have mechanisms in place to ensure that personnel comply with the terms and conditions of employment, including the organization's information security policy and appropriate work practices. It is recommended that these maintenance methods consider the following:

Clarification of information security policy:
Management shall clearly define the organization's information security policy and require personnel to comply with it. The policy should preferably include specific guidelines regarding data protection, access management, security measures, etc.

Inclusion in terms of employment:
Compliance with information security, including information security policies and appropriate work practices, is incorporated as a condition of employment. Personnel should

be required to agree to information security policies when accepting employment contracts and regulations.

Providing education and training:
Personnel should be provided with education programs and training on the information security policy and appropriate methods of working. New employees and personnel in related departments should receive training on the fundamentals of information security and the policy.

Compliance monitoring and evaluation:
Management should periodically monitor compliance with the information security policy and conduct appropriate evaluation. If a violation or issue occurs, appropriate action should be taken and improvements made as necessary.

Rewards and Rewards:
A system of rewards should be introduced for personnel who comply with the information security policy and practice appropriate methods of working, providing certification or benefits for good practice to increase motivation.

Continuous improvement:
Continuously improve information security policies and appropriate work practices, and strive to improve the organization's security level. It is best to constantly adapt to current conditions by leveraging user feedback and industry best practices.

B.3. Management Responsibilities
B.3.6.
Regularly provide education and competency regarding security and cryptographic keys to those responsible for handling data storage systems and to personnel.

Guidance
Regularly provide education and competency regarding security and cryptographic keys to those responsible for handling data storage systems and to personnel. These implementation methods should consider the following:

Formulating an educational program:

The organization shall formulate a security education program for the management and personnel responsible for the Data Storage System. The program should cover everything from basic security principles to the importance of cryptographic keys and how to respond to security threats.

Conducting regular training:
The security education program shall include regularly scheduled training sessions. Training should be provided to help management and personnel deepen their understanding of the latest security methods and best practices.

Strengthening education on cryptographic keys:
The educational program should provide specialized training that focuses on the importance and use of cryptographic keys. Management and personnel should be required to acquire basic knowledge and skills relating to cryptographic key generation, management, and protection.

Conducting practical simulations:
The Security education program shall include practical simulations and exercises. Management and personnel to improve their ability to respond to actual security events through these simulations.

Providing assessment and feedback:
The security education program shall include a mechanism to periodically assess participants' understanding and ability and to provide feedback. Feedback from participants should be used to improve the education program.

Continuous learning and improvement:
The organization shall provide resources to help management and personnel continuously learn and improve, supporting access to information on the latest security trends and technologies to help build expertise.

B.3. Management **Responsibilities**

B.3.7.

Management of the Data Storage System management organization should establish a mechanism to provide personnel with an anonymous reporting channel to report violations of information security policies or procedures (for example, whistleblowing).

Guidance

Management of the Data Storage System management organization should establish a mechanism to provide personnel with anonymous reporting channels to report violations of information Security policies or procedures, such as whistleblowing. The following items should be considered when establishing this mechanism.

Establishment of anonymous reporting channel:
Management should establish a dedicated reporting channel for anonymously reporting violations of information security policies or procedures. This channel should ensure strict confidentiality and anonymity so that personnel can report violations with confidence.

Clarification of reporting procedures:
The procedure and method for anonymous reporting channels should be clearly defined and communicated to personnel. Information about the reporting channel should be posted in an appropriate location within the organization so that personnel can easily access it.

Protection of reporters:
Measures should be taken to protect the anonymity of reporters. Management should take appropriate measures to ensure reporters can make reports without fear of retaliation or disadvantage.

Processing and investigation of reports:
Submitted reports should be handled appropriately, and prompt and fair investigation conducted as necessary. The response to reports should remain transparent and be appropriately communicated to interested parties.

Feedback to reporter:

Anonymous reporters should be given feedback confirming that their report was received and on the status of the response.
Appreciation should be expressed to reporters, demonstrating the organization's proactive stance toward reporting.

Continuous improvement and transparency:
The effectiveness and transparency of the anonymous reporting channel should be continuously evaluated and improved. Management should periodically publicize the existence and activity of the reporting channel, both internally and externally, to ensure transparency.

B.3. Management **Responsibilities**

B.3.8.

Management of data storage systems management organizations should demonstrate support for and lead by example for information security policies, procedures, and controls.

Guidance

Management of Data Storage Systems management organizations should demonstrate support for information security policies, procedures, and controls, and act as a role model. The following items should be considered with regard to these actions.

Clarification of policies and procedures:
Management should clearly define policies, procedures, and controls regarding information security and encourage compliance within the organization. Policies and procedures should include specific guidance regarding data storage, access management, security policy compliance, etc.

Demonstration of support:
Management shall demonstrate support for information security policies and procedures through actions. Management should ensure that policies and procedures are followed through active involvement in information security and the implementation of appropriate measures.

Transparency and communication:

Management should ensure transparency regarding information security policies and procedures and encourage communication with employees. It is advisable to clearly explain the purpose and importance of policies and procedures and to help employees understand their importance and comply with them.

Leadership implications:
Management should demonstrate leadership regarding information security and serve as a positive role model for employees. Management should emphasize its commitment to policies and procedures through regular reporting on information security challenges and successes.

Continuous evaluation and improvement:
Management shall continually evaluate the effectiveness of information security policies and procedures and make improvements as necessary.
The policies and procedures should be periodically reassessed to respond to new threats and technological developments and to raise the organization's overall security level.

B.4. Contractor management

B.4.1.

The management of the Data Storage System shall confirm through the policy set, procedures, and controls for information security that another organization to which work related to key information and encrypted data and system configuration is outsourced has the following in place for workers.

- **Mechanism to provide guidelines for demonstrating information security expectations in roles within the organization**
- **Mechanism to motivate the organization to follow a set of policies for information security**
- **Mechanism to achieve a certain level of awareness of information security related to one's role and responsibility within the organization**
- **Mechanisms to ensure compliance with terms and conditions of employment, including the organization's information security policy and appropriate work practices**
- **Mechanism to maintain appropriate skills and qualifications and receive regular training**
- **Mechanisms that provide anonymous reporting channels (e.g. whistleblowing) for reporting violations of information security policies or procedures;**

Guidance

The management of the Data Storage System shall establish a mechanism for other organizations to which work related to key information and encrypted data and system configuration are outsourced to provide guidelines to personnel to demonstrate expectations regarding information security. The following items should be considered in confirming this.

Providing guidance:

Ensure that the other organization provides guidance to personnel setting out their roles and expectations regarding information security. This should ensure that personnel understand their roles and are expected to adhere to appropriate security practices.

Motivation mechanism:

Confirm that a mechanism is in place to motivate other organizations and personnel to comply with information security policies. Ideally, this will include incentive systems, educational programs, and appropriate feedback mechanisms.

Increased awareness:
It should be confirmed that the other organization has established a mechanism to motivative its personnel to comply with information security policy, including reward mechanisms, education programs, and appropriate feedback mechanisms.

Compliance with employment conditions:
It should be confirmed that the other organization has established terms and conditions of employment to ensure its personnel comply with information security policy and appropriate work procedures, including contracts, rules, and internal regulations.

Education and qualifications provided:
Ensure that other organizations and personnel have appropriate skills and qualifications and provide a mechanism for regular information security training. This encourages personnel to stay informed about the latest security practices and technologies.

Providing anonymous reporting channels:
Verify that another organization provides an anonymous reporting channel for reporting violations of information security policies and procedures. This should make it easier for personnel to report security concerns and issues anonymously.

B.5. Data storage area to be encrypted and erased
B.5.1.
Documented information shall be prepared that clearly states the data storage area and subject to cryptographic erasure.

Guidance
For the data storage area to be encrypted and erased, documented information shall be prepared that clearly states the data storage area and subject to cryptographic erasure. The following items should be considered in documenting this.

Clear definition of data storage areas:

The organization shall create documented information that clearly defines the data storage areas and scope that will be subject to cryptographic erasure. This documented information should preferably include information such as what data is covered, what format it is stored in, and where it is stored.

Detailed description of target data:
The documented information shall provide a detailed description of the data subject to cryptographic erasure, including data type, format, retention period, and access right of the data.

Clarification of scope:
The scope of the data storage area is clearly defined and explained in detail in the documented information, clearly identifying what is included in scope, such as specific servers, databases, file systems, and cloud storage.

Clarification of management responsibilities:
The documented information should clearly indicate the management responsibility for the data storage area, clearly defining who is responsible and what kind of authority and responsibility they have.

Update and review process:
The documented information should define a process for regular updates and review. When new data storage area is added or a change occurs, the documented information should be updated and reviewed as necessary

Access control and monitoring:
Documented information should include policies regarding access control and monitoring of data storage area, clearly defining access rights management, log monitoring, detection of unauthorized access.

Compliance with legal and regulatory requirements:
Documented information shall be designed to comply with legal and regulatory requirements. Legal and regulatory requirements relating to data storage areas should be included and measures taken to comply should be clearly stated.

B.5. Data storage area to be encrypted and erased

B.5.2.

The following shall be stated regarding the encryption used.

• the encryption layer

• the encryption algorithm

• the method of the key acquisition

• the Key retention period

• the method of Key protection

The encryption algorithm used shall be one listed in the CRYPTREC List.

Guidance

For encryption used in the data storage area subject to cryptographic erasure, it should be used the encryption algorithm to be one listed in the CRYPTREC List, and the following items should be considered.

Encryption layer:

The encryption layer used should be clearly specified. Transport-layer encryption (such as TLS) should be typically used when data is in transit.

Encryption algorithm:

The encryption algorithm used should be clearly stated. An algorithm listed in the CRYPTREC List should be selected.

The method of key acquisition:

The method for acquiring the key used for encryption should be clearly defined, including the method of key generation or exchange and the management procedure.

Key retention period:

The key retention period should be specified, clearly defining the key's expiration and how frequently it is regenerated.

Method of key protection:

The method of key protection should be specifically described, including where the key is stored, access rights, backup methods, and physical protection.

Use of CRYPTREC-listed encryption algorithms:
It should be clearly stated that an encryption algorithm listed in the CRYPTREC List is used for encryption, since the CRYPTREC List includes highly reliable encryption algorithms.

Compliance with legal and regulatory requirements:
Ensure compliance with legal and regulatory requirements regarding encryption. The choice of encryption method and key management method should depend on the regulatory requirements of a particular industry or country.

Audit and evaluation:
Regular audits and evaluations of encryption implementation and operation should be conducted to identify security vulnerabilities or areas for improvement and take countermeasures as necessary.

B.5. Data storage area to be encrypted and erased

B.5.3.

Data to be stored shall be automatically encrypted before being written to non-volatile media.

Guidance

The data stored in the data storage area shall be automatically encrypted before being written to a non-volatile medium. The following items should be considered in doing so.

Implementation of automatic encryption:
An automatic encryption system should be implemented before writing data to non-volatile media. Systems should be configured to automatically perform encryption before data is stored.

Choosing an encryption algorithm:
The encryption algorithms used should be carefully selected. balancing security and performance to choose a highly reliable encryption method.

Key generation and management:

The keys used for encryption shall be automatically generated or appropriately managed. Keys used over a long period should be updated periodically.

Cryptographic transparency:
Automatic encryption should be transparent to users and applications, and should be designed to have no impact on data write and read operations.

Protection of cryptographic keys:
Keys used for encryption shall be appropriately protected. Strict security measures for key storage and access control should be implemented to prevent unauthorized access and data leaks.

System monitoring and management:
The automated encryption system shall be monitored and appropriately managed during operation. If an error or anomaly is detected, immediately upon detection.

The automatic encryption system should be monitored and appropriately managed during operation, with errors or anomalies addressed immediately upon detection.

Continuous improvement:
Automated encryption implementations are subject to continuous improvement. Systems should be regularly reviewed and updated to keep pace with technological advances and security threats.

B.6. Encryption Settings before Data Storage

B.6.1

It shall be clearly stated in the policy or procedure that unencrypted data shall not be stored in the area designated for encryption.

Guidance

It shall be clearly stated in the policy or procedure that unencrypted data shall not be stored in the area designated for encryption. The following items should be considered in doing so.

Purpose of data encryption:

Encryption is preferably a means of ensuring confidentiality and increasing protection of data.

Definition of the area designated for encryption
The area designated for encryption should refer to the area where data requiring confidentiality protection is stored.

Policy statement:
Policies or procedures should clearly state that unencrypted data is not stored in encrypted areas. Storing data before encryption can lead to confidentiality violations and security risks.

Handling of data before encryption:
Unencrypted data shall be properly erased or stored after encryption is applied. It should be noted that unnecessarily retaining unencrypted data may lead to breaches of confidentiality and legal compliance.

Selection of an appropriate encryption method:
An appropriate encryption method should be selected to protect confidentiality. noting that the selection of encryption techniques should be based on requirements for data confidentiality, performance, and cost.

Regular audits and evaluations:
Policies and procedures for encrypted areas are verified through regular audits and evaluations. Regular audits should be conducted to gain insight into policy enforcement and security risks.

B.6. Encryption Settings before Data Storage
B.6.2.
It shall be confirmed and recorded at the time of commencement of use, that no data is stored in the area designated for encryption. “Commencement of use” refers to the date and time when automatic encryption settings was applied to the area designated for encryption.

Guidance

It shall be confirmed and recorded at the time of commencement of use, that no data is stored in the area designated for encryption. “Commencement of use” refers to the date and time when automatic encryption settings was applied to the area designated for encryption. The following items should be considered in doing so.

Definition of start of use of encrypted area:
The start of use of the encryption target area preferably refers to the date and time when the encryption settings are automatically applied and the encryption target area becomes usable.

Check and record at commencement of use
At the time of commencement of use, it should be confirmed and recorded that no data is stored in the area designated for encryption. This should be confirmed by auditing or scanning the contents of the area, as this confirmation and record is important for security transparency and accountability.

Record contents:
The checks and records performed at the start of use should include the following information:
• Usage start date and time
• Name or identifier of the area to be encrypted
• Data storage status (if it is confirmed that the data does not exist, clearly state that fact)
• Name or identifier of the person in charge of the confirmation

Storage of records:
Confirmations and records from the start of use should be kept in accordance with appropriate security standards. Records should be easily accessible to respond to audits and legal requests as necessary.

Periodic reconfirmation:
The contents of the area designated for encryption should continue to be audited periodically after commencement of use to confirm that data continues to be properly encrypted. Such reconfirmation is important for ensuring ongoing security and compliance with the policy.

B.7. Restrict retention of cryptographic keys outside the Key Management System

B.7.1.

The Data Storage System shall not retain cryptographic keys in a non-volatile state. Note:If this requirement cannot be met, the alternative measures in B.8.8 through B.8.10 shall be applied instead.

Guidance

In a Data Storage System that restricts the retention of cryptographic keys outside the Key Management System, The Data Storage System shall not retain cryptographic keys in a non-volatile state. The following items should be considered in doing so.

Keeping cryptographic keys in a non-volatile state:
To avoid holding cryptographic keys in a non-volatile state in order to improve encryption strength and key security, the Data Storage System should not retain cryptographic keys in a non-volatile state.

Temporary use of keys:
Cryptographic key should be loaded into memory temporarily and used only as needed. After a cryptographic key has been used, the key should be erased from memory as soon as possible.

Generate and exchange cryptographic keys:
The cryptographic key is randomly generated using a secure random number generator. The exchange of cryptographic keys is preferably performed via a secure communication path or key exchange protocol.

Storage of cryptographic keys:
Cryptographic keys are stored using a security mechanism such as a secure Key Management System or hardware security module (HSM). Cryptographic keys should be protected from physical and unauthorized access.

Periodic rotation of cryptographic keys:

Cryptographic keys should be rotated regularly to maintain key strength and security. following a regular schedule based on security policy.

Proper deletion of keys:
Cryptographic keys that are no longer needed shall be deleted using an appropriate method. Since key deletion is important for minimize the risk of leakage of confidential information and security risk.

B.8. Access Control
B.8.1.
Work with key information and encrypted data, and the assignment of privileges for system configuration, shall be managed through a formal authorization process in accordance with relevant access control policies.

Guidance
For access control, operations related to key information and encrypted data, and assignment of privileges for system configuration should be managed through a formal authorization process in accordance with the relevant access control policy, and the following should be considered.

Compliance with access control policies:
Authority for work related to key information and encrypted data, and for system configuration, should strictly follow the relevant access control policy.

Formal approval process:
Changes to work related to key information and encrypted data, or to system configuration, should be managed through. A formal authorization process should be approved by an appropriate administrator or responsible person.

Assigning access rights:
Access rights necessary to perform tasks or system configurations related to keying material or encrypted data should be assigned in accordance with the principle of least privilege, granting only the minimum necessary rights.

Review and update access rights:

Access rights should be reviewed regularly and updated as necessary. Reviews should be based on changed roles, business requirements, and security risks.

Audit and traceability:
Activities related to key information and encrypted data and changes to system configurations shall be performed in an auditable and traceable manner. All changes should be appropriately logged and audited if necessary.

Education and awareness:
Appropriate training and awareness opportunities will be provided to staff involved in the management of key information and encrypted data. Staff should be educated about the importance of following security and access control policies.

B.8. Access Control
B.8.2.
Privileges for working with keys, encrypted data, and configuring systems are assigned based on the minimum requirements of the user's job role.
It is preferable that the account to which system configuration privileges are assigned be linked to an individual user, and that system configuration privileges should not be assigned to an account that is shared by multiple users.

Guidance
Access controls ensure that privileges for working with key information, encrypted data, and system configuration are assigned based on the minimum requirements for the user's job role. It is recommended that the account to which system configuration privileges are assigned be linked to an individual user, and that system configuration privileges should not be assigned to an account that is shared by multiple users. The following items should be considered.

Assign privileges based on minimum requirements:
Authority for work related to key information and encrypted data and systems configuration should be assigned based on the minimum requirements of the user's job role, granting only the authority necessary and following the principle of least privileges.

Use of individually linked accounts:

The account to which system configuration privilege is assigned shall be an individual account linked to a specific user. By using accounts linked to individuals, the actions of a specific user should be fracked and be clear where responsibility lies.

Avoiding privilege assignment in shared user accounts:
System configuration privilege should not be assigned to accounts shared by multiple users. Since shared user accounts make it difficult to manage individual user access and traceability of individually linked accounts is recommended instead.

Defining privileges according to role:
Appropriate privileges should be defined according to each user's role and responsibility, with reassessment and adjustment of authority as users' roles or duties change.

Review and update permissions:
Permissions should be reviewed regularly and updated as necessary. Reviews should be based on changed roles, business requirements, and security risks.

B.8. Access Control
B.8.3.
If a user assigned the authority to work on key information, encrypted data, or system configuration is replaced due to personnel changes or retirement, access rights shall be changed or deleted.

Guidance
Regarding access control, if a user who has been assigned the authority to work on key information, encrypted data, or system configuration is replaced due to personnel changes or retirement, it shall change or delete access rights, and The following items should be considered.

Managing access rights due to personnel changes or terminations:
If a user assigned authority to work on key information or encrypted data or to configure system configuration is replaced due to personnel changes or retirement, it shall change or delete access rights immediately.

Change steps:

Change or delete access rights by following the prescribed procedures. Change procedures should be in accordance with organizational policies and procedures and should obtain necessary approvals.

Change access rights:
When a user is replaced due to personnel changes or retirement, appropriate access rights should be assigned to the new user. Appropriate privileges should be granted to new user according to their roles and responsibilities.

Revoking access rights:
The former users' access rights shall be promptly revoked. The revocation procedure should be performed in accordance with information security policy and access control policy.

Ensuring traceability:
The process of changing or erasing access rights shall be appropriately recorded to ensure traceability, including the reason for the change, the person who carried it out, and the date and time.

Audit and review:
The process for changing or erasing access rights shall be regularly audited and reviewed as necessary. Audits and reviews should preferably confirm that changes and deletions of access rights are being implemented appropriately.

B.8. Access control
B.8.4.
Users and systems assigned privileges for working with key information, encrypted data, and system configuration are reviewed at regular intervals.

Guidance
For access control, users and systems assigned privileges for work related to key information and encrypted data, and system configuration shall be reviewed at regular intervals, and the following items should be considered.

Define review frequency:

Users and systems assigned privileges for working with key information and encrypted data and configuring systems should be reviewed at regular intervals. Review intervals should be defined based on security policy and industry best practices.

Reviewed for:
The review should include all users and systems with authority to work with key information, encrypted data, or configure system configuration. The scope of review should be clearly defined by administrators and security teams.

Review steps:
Reviews should be conducted in accordance with prescribed procedures. Review procedures should include checking access rights, assessing suitability of rights, and detecting unauthorized access.

Assessing the need for change:
If, as a result of the review, changes or updates to access rights are necessary, appropriate procedures will be followed to implement the changes. If changes are required, a formal approval process should be followed before the changes are implemented.

Ensuring traceability:
The review process and results shall be appropriately recorded and traceability shall be ensured. It should record information such as who conducted the review, the results, and why changes were required.

Implementation of improvements:
Appropriate improvement measures shall be implemented based on the results of the review. Remediation measures should be implemented in accordance with security policies and industry best practices.

B.8. Access control
B.8.5.
Records all work with key information, encrypted data, and authorizations assigned to system configuration privileges.

Guidance

For access control, all operations related to key information and encrypted data, as well as all authorizations assigned to system configuration privileges, should be recorded and the following items should be considered.

Authorization record:
When assigning privileges for tasks related to keying information, encrypted data, or system configuration, all authorizations shall be formally recorded. Authorization records should be assigned information such as who received what authority and the date and time the authority.

Record contents:
Records should preferably include the following information:
• User or system identifier
• Assigned privileges and roles
• Permission expiration date (if necessary)
• Authority assignment date and time
• Identifier of the administrator who gave the authorization

Storage of information:
Records of approval shall be kept securely. Records should be kept in a location with appropriate access controls in accordance with the highest standards of information security.

Record tracking:
Approval records shall be maintained appropriately to track change history. When records are changed, the nature and reason for the change should be properly documented information.

Audit and traceability:
Records of authorization shall be subject to periodic audits and security verification. Audits of records should ensure that privilege assignments are properly implemented and comply with security policies.

B.8. Access control

B.8.6.

Do not allow any work with key information, encrypted data, or system configuration until the authorization process is complete.

Guidance

Access control should preferably not allow operations on key information, encrypted data, or system configuration until the authorization process is complete, and the following items should be considered.

Prohibited work:

Operations related to key information, encrypted data, and system configuration should be prohibited until the authorization process has been completed.

Starting the authorization process:

Before working with key information, encrypted data, or changing system configuration, begin the authorization process. The authorization process should include procedures for obtaining necessary approvals.

Obtaining approval:

Obtain approval from appropriate management and/or interested parties to obtain approvals related to changes to work or system configuration. Approval should preferably be done in a manner that complies with security policies and regulatory requirements.

Process completed:

Once the necessary approval has been obtained, the work or system configuration change may be carried out. Work should not be permitted until the authorization process is complete and all related procedures and approvals have been established.

Audit and traceability:

Until the approval process is completed, information regarding the process of prohibiting work and obtaining approval should be appropriately recorded and traceability ensured. For audit purposes, relevant information should be made available as needed.

Compliance and education:

Educate all parties on the importance of work prohibitions and approval processes and comply with them. It should promote understanding of how to carry out appropriate procedures through appropriate education and awareness-raising activities.

B.8. Access control

B.8.7.

<Alternative requirements when HYOK cannot be implemented>

Apply controls to prevent anyone from accessing or manipulating key information without authorization or detection.

Specific control measures include monitoring of operation logs, two-person work rules, division of password knowledge, and work after approval by the administrator.

Guidance

Access control is the application of management measures to prevent unauthorized or undetected access or manipulation of key information by a single person. As for specific control measures, it should consider monitoring of operation logs, two-person work rule, division of password knowledge, work after approval by the administrator, etc., and the following items should be considered.

Access and operation restrictions:

Even if HYOK cannot be implemented, it should apply control measures to prevent unauthorized or undetected access or manipulation of key information by anyone.

Specific control measures:

The following controls should be considered.

- Monitoring of operation logs: Monitoring of operation logs to detect unauthorized access or operations when key information is accessed or manipulated.
- Two-person work rule: Important operations and changes to key information shall be performed by two people with the approval and supervision of two or more people.
- Password knowledge division: Dividing the passwords required to access key information among multiple parties and keeping them so that no one can access them alone.
- Work after approval by the administrator: Important operations or changes to key information require approval by the administrator, and the work is executed after approval.

Proper monitoring and traceability:
If alternative requirements are applied, access and operation logs will be appropriately monitored and any unauthorized access or operation will be promptly addressed. Logs should be stored appropriately and provided for audits and investigations as necessary.

Regular evaluation and improvement:
The effectiveness of alternative requirements shall be periodically evaluated and improved as necessary. Improvements should be made based on security risks and business requirements.

B.8. Access control **B.8.8.** **<Alternative requirements when HYOK cannot be implemented>** **Separate users who are assigned privileges for working with key information and encrypted data and system configuration, and those who authorize those**

Guidance
For access control, it should separate users who are assigned the authority to work on key information and encrypted data and system configuration from those who authorize that authority, and the following items should be considered.

Separation of user and authorizer:
It should clearly separate the users who are assigned the authority to work on key information, encrypted data, and system configuration, and the person who authorizes that authority.

Separation of roles and responsibilities:
Clearly define the roles and responsibilities of users and authorizers to avoid confusion. Users perform tasks and operations, and an authorizer should play the role of approving those tasks and operations.

Implementation of the approval process:
Implement appropriate authorization processes before assigning new privileges to users. The authorization process should include procedures for obtaining necessary approvals.

Authorization clarification:
When a user obtains a new privilege, the person granting the privilege is clearly identified. Approvers should have appropriate authority and roles and responsibilities that are clearly defined.

Establishment of dual management system:
Establish a dual governance structure to strengthen the separation of users and authorizers. Significant operations and changes should be approved by multiple parties.

Audit and traceability:
Conduct periodic audits to ensure proper separation of users and authorized persons. Audit results should be appropriately recorded and traceability ensured.

B.8. Access control
B.8.9.
<Alternative requirements when HYOK cannot be implemented>
When users or administrators work on key information or encrypted data or perform system configuration, create control measures to prevent fraud by monitoring activities, audit trails, and supervision by management.

Guidance
For access control, when users or administrators work on key information or encrypted data or perform system configuration, it should develop control measures to prevent fraud by monitoring activities, audit trails, supervision by management, etc., and and the following items should be considered.

Monitoring activity:
Monitor user or administrator activities in real time as they work on key information, encrypted data, or configure system configuration. It should detect fraud or abnormal activity early through monitoring and take appropriate action.

Creating an audit trail:
Creating an audit trail of logs and events generated by monitoring activities. The audit trail should include information such as who did what and when.

Management oversight:

The management layer supervises user activities and administrator actions to prevent fraud. Oversight should preferably include periodic reviews and reports, as well as investigations and responses as necessary.

Rapid response to fraud:
If fraudulent activity is detected through monitoring or analysis of audit trails, respond promptly. It should identify the source of fraud and take appropriate measures to minimize damage.

Training and education:
Provide training and education to users and administrators regarding fraud prevention. It should strive to improve security awareness and disseminate appropriate codes of conduct.

Regular audits and improvements:
Conduct periodic audits and evaluations to confirm the effectiveness of controls. It should improve security levels by improving controls and processes based on audit results.

B.8. Access control **B.8.10.** **<Alternative requirements when HYOK cannot be implemented>** **Controls to prevent fraud are in place.**

Guidance
For access control, it should implement management measures to prevent fraud, and the following items should be considered.

Operation of controls to prevent fraud:
Confirm that controls to prevent fraud are being operated appropriately. Controls should be developed and implemented based on the organization's security policy and regulatory requirements.

Clarification of control measures:
Controls to prevent fraud should be clearly documented and communicated to interested parties. Documented information control measures should clearly state the purpose, targets, procedures, and responsible personnel.

Definition of operational procedures:
Procedures for operating controls to prevent fraud are clearly defined. The operational procedures should describe who is responsible and what processes and tools will be used to implement them.

Regular evaluation and improvement:
The effectiveness of controls to prevent fraud should be periodically evaluated. It should improve controls and processes as necessary based on the results of the evaluation.

Training and awareness:
Appropriate training and awareness activities are carried out so that interested parties understand how to identify and report fraud. Awareness activities should focus on the latest security threats and best practices.

Reporting and prompt response:
In the event of misconduct, those involved should know the appropriate reporting procedures and be dealt with promptly and appropriately. Processes for reporting and responding to misconduct should be properly documented and communicated.

B.9. Change management

B.9.1.

Change management rules and procedures have been established and approved by the responsible person and those responsible for development and maintenance.

Guidance

For change management, change control rules and procedures should be established and approved by the person in charge and the person responsible for development and maintenance, and the following items should be considered.

Develop change management rules:
Change management rules should comprehensively define procedures for requesting, approving, implementing, monitoring, and evaluating changes. Rules should be developed to align with the organization's vision, goals, and security policies.

Defining change control procedures:
Change management procedures should specifically indicate a series of steps from change request to approval, implementation, and evaluation. The procedures should include who requests changes, how approval will be obtained, implementation and testing methods, and how changes will be evaluated.

Appointment of responsible person:
Persons responsible for change control rules and procedures should be clearly designated. A responsible person should be responsible for each stage of change requests, approval, implementation, monitoring, and evaluation.

Approval of development/maintenance manager:
Change control rules and procedures shall be approved by those responsible for development and maintenance. Changes should be made according to approved procedures to ensure consistency and safety.

Documented information changes:
Important decisions and activities at each stage of change management are appropriately documented information. Documented information should include change requests, approvals, implementation procedures, test results, evaluation reports, etc.

Monitoring and evaluation:
Regular monitoring and evaluation should occur even after changes have been implemented. It should appropriately evaluate the impact and outcomes of changes and improve procedures and processes as necessary.

B.9. Change management
B.9.2.
When change management requests occur, the impact on other systems shall be considered.

Guidance
For change management, when a change management request occurs, it should consider the influence of other systems, and the following items should be considered.

Evaluation of change requests:
When a change management request occurs, first assess the impact on other systems. In order to accurately understand the scope of impact, it should clearly identify other related systems and services.

Analysis of impact area:
Detailed analysis of the impact of changes on other systems. The scope of impact should preferably include data integrity, system availability, and impact on related processes and workflows.

Collaboration of interested parties:
Work closely with other system owners and interested parties involved in the change management process. It should share information on the scope of impact and change plans, and make necessary agreements and adjustments.

Coordinating change plans:
Adjust change plans appropriately, taking into account the impact on other systems. It should consider the timing and procedures of changes, test plans, etc. so that they are in harmony with other systems.

Implement and monitor changes:
When changes are implemented, monitor the impact on other systems. If the impact of a change is likely to expand unexpectedly, it should take countermeasures quickly.

Risk management:
Appropriately manage risks related to changes, taking into account the impact on other systems. It should consider preventive measures and workarounds to minimize risks and modify change plans as necessary.

B.9. Change management
B.9.3.
Emergency change requests are documented and change control procedures are followed.

Guidance

For change management, urgent change requests should be documented and change control procedures should be followed, and the following should be considered.

Documented information requirements:
In the event of an emergency change request, the request shall be appropriately documented. Documented information should include the reason for the change, its scope, impact, and how it will be implemented.

Follow change control procedures:
Emergency change requests should be subject to the same change control procedures as regular changes. Change control procedures should include steps such as request submission, evaluation, approval, implementation, monitoring, and evaluation.

Clarifying priorities:
The priority of urgent change requests is clearly defined. Priorities should be set taking into account the importance, urgency, impact, etc. of changes.

Prompt response:
Urgent change requests shall be responded to promptly. Prompt judgment and action should be required at each stage of the change control procedure.

Proper documented information:
Even after emergency change requests are approved, they are properly documented. The details, results, and impacts of implemented changes should be appropriately recorded and traceability be ensured.

Monitoring and evaluation:
After emergency changes are implemented, the impact and outcomes of the changes are appropriately monitored and evaluated. If inappropriate changes or impacts occur, it should deal with them promptly.

B.10. System clock

B.10.1.

Prepare a mechanism to ensure the time accuracy of the system clock within the system using time synchronization technology.

Guidance

It should provide a mechanism for ensuring the time accuracy of the system clock within the system using time synchronization technology, and the following items should be considered.

Selection of time synchronization technology:
Select an appropriate time synchronization technique to ensure the time accuracy of the system clock. It is preferable to use technologies such as NTP (Network Time Protocol) and PTP (Precision Time Protocol).

Setting up a time synchronization server:
Install a time synchronization server in an appropriate location to use time synchronization technology. The server should be highly reliable and easily accessible to the network.

Client settings:
Setting up a connection to a time synchronization server for clients (servers, workstations, etc.) in each system. the client periodically should obtain time information from the time synchronization server and synchronize the system clock.

Security considerations:
Consider the security of time synchronization technology. It should take security measures such as encrypting and authenticating time synchronized communications.

Monitoring and alerts:
Monitor the status of time synchronization and send appropriate alerts if anomalies are detected. Time synchronization failures and delays should be addressed as soon as possible.

Regular evaluation and adjustment:
Perform periodic evaluation and adjustment to maintain accuracy and reliability of time synchronization. It should monitor the time difference between the system clock and the time synchronization server and make adjustments as necessary.

B.10. System clock

B.10.2.

The time accuracy of the system clock within the Data Storage System is maintained using time synchronization technology.

Be able to check the time synchronization settings and sampled logs for the above.

Guidance

The system clock shall use time synchronization technology to maintain the time accuracy of the system clock within the Data Storage System. It should be able to check the time synchronization settings and sampled logs, etc., and the following items should be considered.

Selection of time synchronization technology:
Selecting appropriate time synchronization techniques to ensure the time accuracy of system clocks within data storage systems. It should select highly reliable technologies such as NTP (Network Time Protocol) and PTP (Precision Time Protocol).

Build time synchronization settings:
Make appropriate settings to use time synchronization technology. It should ensure that all data storage systems in the system are properly connected to the time synchronization server.

Logging and monitoring:
Recording logs for monitoring time synchronization settings and system clock status. The log should include time synchronization events, system clock change history, and the like.

Regular checks and audits:
Regularly check time synchronization settings and logs to ensure that system clock time accuracy is maintained. It should conduct an audit to confirm whether the settings are being implemented appropriately.

Setting up alerts:

If an abnormality or problem with time synchronization is detected, settings should be made so that appropriate alerts are sent. alerts should allow problems to be detected and dealt with promptly.

Preparation for troubleshooting steps:
Have appropriate troubleshooting steps in place in case time synchronization issues occur. The procedure should include how to identify the problem and how to resolve it.

C. Encryption System

C. Encryption System

C.1.Security Policy

C.1.1.

The Key Management System management organization shall establish a security policy to protect data. The following shall be clearly stated in the security policy.

a) Appropriate for the purpose of the organization.

b) include information security objectives or provide a framework for setting information security objectives;

c) includes a commitment to meeting applicable requirements related to information security;

Guidance

A information security policy expresses the organization's top-level approach to encryption and cryptographic erasure as part of an Encryption System. From this perspective, it should formulate a security policy that takes the following into account.

Ensuring suitability:

The information security policy should be appropriate to the organization's objectives and consistent with the objectives of the Key Management System.

Clarification of information security objectives:

The information security policy should clearly state the purpose of information security and provide a framework for the Key Management system to protect data and ensure its confidentiality and integrity.

Statement of commitment:

The security policy should include an organization-wide commitment to meeting applicable information security requirements. Organizations should commit to providing the resources and support necessary to implement and comply with security policies.

Defining access control policy:

The security policy clearly defines access control requirements for key information and encrypted data. These requirements should include authentication, authorization, and auditing processes, as well as appropriate procedures to maintain confidentiality.

Change management and auditing:
The security policies should define change management processes and provide mechanisms for addressing changing security requirements and new threats. Audits and evaluations of policies should be conducted on a regular basis to ensure that policies are being effectively and appropriately implemented.

Education and awareness:
Security policies provide resources and programs to educate the interested parties both inside and outside of the organization. It is important that all interested parties understand and comply with the security policy, which should provide appropriate training and information.

C.2. System Configuration, and Organizational Structure, Roles

C.2.1.

Encryption system management organizations shall prepare documented informations that can confirm the roles, responsibilities, and systems of their own workers who perform work related to key information and encrypted data and system configuration, or of other organizational Structure to which work is

Guidance

The system configuration, structure, and roles are to clarify the system structure, structure, and role in cryptographic erasure as an Encryption System management organization. It should clarify the system configuration, structure, and roles in various regulations, organizational charts, etc. From this perspective, it should clarify the system configuration, structure, and roles by considering the following.

Clarification of roles and responsibilities:
Encryption System management organization shall clearly define the roles and responsibilities of their own personnel who perform work related to key information and encrypted data, as well as the roles and responsibilities of other organizations to which work is outsourced. For each worker or organization, it should prepare documented information that includes the work content, scope of responsibility, contact information, etc.
System development:
The Encryption System management organization will develop an appropriate system for handling key information and encrypted data and configuring the system. The structure should include necessary resources, authority, oversight, contact information, etc.

Documented Information Creation:
The organization should create documented information identifying the roles, responsibilities, and organizational structure related to handling key information and encrypted data and configuring the system. The information should be easy to understand, sufficiently specific, and stored in a location that is readily accessible to interested parties.

Regular reviews and updates:
The documented information should be reviewed regularly and updated as necessary. When changes occur to the contents of documented information such as when changes are made or new personnel are added, it should update the documented information promptly.

Notification and Education of Interested parties:
To appropriately notify and explain documented information regarding work and systems related to key information and encrypted data to related parties are essential. It should provide the necessary education and training to ensure that those interested parties understand their roles and responsibilities and are able to carry out their duties appropriately.

C.2. System configuration, structure, roles

C.2.2.

The Encryption System management organization shall prepare documented information that can confirm the configuration and data flow of the system that handles key information and encrypted data, and its surrounding environment.

Guidance

The Encryption System management organization shall prepare documented information that can confirm the configuration and data flow of the system that handles key information and encrypted data. It should clarify this documented information using a configuration diagram of the relevant system. From this perspective, it should document the configuration and data flow of the system which handles key information and encrypted data can be confirmed in consideration of the following.

Clarification of system configuration:
The organization responsible for managing the encryption system shall clearly document the configuration of all systems that process, store, or transmit cryptographic keys and encrypted data. The documentation should include, at a minimum, the relevant hardware, software,

network architecture, system interfaces, and security configurations.

Data flow description:
To describe the data flow related to handling of key information and encrypted data, it is necessary that the procedures and processes from data generation source to storage, processing, transfer, and deletion to be clearly described.

Description of security measures:
The documented information should include security measures related to system configuration and data flow. It should include specific measures to strengthen security, such as access control, encryption, and audit log settings.

Description of integration and dependencies between systems:
Clearly explaining how the system that handles key information and further encrypted data is integrated with other systems. However, it will be on case of if there are any dependencies. It should show how to exchange data with other systems and how to share data.

Documented information updates and reviews:
Documented information should be reviewed regularly and updated as necessary. It is necessary that the documented information be updated appropriately when there are changes or upgrades to the system, or the addition of new security requirements.

Sharing and educating interested parties:
Ensure that documented information related to system configuration and data flow are appropriately shared and understood by interested parties. It is advisable to provide appropriate education and training so that interested parties can understand the system configuration and data flow, and understand the importance of security

C.3. Management Responsibilities

C.3.1.

The management of the Encryption System management organization shall establish a mechanism to appropriately communicate key points regarding information security roles and responsibilities before workers are allowed to work on key information, encrypted data, or access system configuration.

Guidance

The management of the Encryption System management organization shall establish a mechanism to appropriately communicate key points regarding information security roles and responsibilities before personnel are allowed to work on key information, encrypted data, or access system configuration. Possible ways to prepare this information include creating a role/responsibility table. When developing these roles and responsibilities, it should consider the following:

Clarification of management roles and responsibilities:
Management should understand the importance of information security and recognize its responsibility. It should be responsible for developing and maintaining information security policies.

Education and training for personnel:
Regularly educate and train personnel on the importance and responsibility of information security. It should provide guidelines on how to handle key information and encrypted data and on access privileges to the system.

Dissemination of information security policy:
Disseminate the information security policy within the organization and ensure that all personnel understand and comply with it. If there are any updates or changes to the policy, it is advisable to communicate them appropriately and confirm understanding.

Enhanced access control:
Access to key information and encrypted data should be restricted to the minimum necessary privileges. It is essential that personnel who have been given access authority work only within the scope of their authority.

Audit and evaluation:
Regularly audit information security implementation status and evaluate compliance status. Based on the audit results, it should identify areas for improvement and take appropriate measures.

Risk management and response:
Assess risks related to information security and develop appropriate controls. When a

security incident occurs, it should respond promptly and take appropriate measures.

Continuous improvement:
Continually improve information security policies and procedures to keep up with the latest threats and best practices. It should foster a culture in which all members of the organization cooperate in improving information security.

.

C.3. Management Responsibilities
C.3.2.
The management of the Encryption System management organization shall establish a system to provide guidelines to workers to indicate their expectations regarding information security in their roles within the organization.

Guidance
The management of the Encryption System management organization shall establish a system to provide guidelines to personnel to indicate their expectations regarding information Security in their roles within the organization. It is recommended that these maintenance methods consider the following:

Executive leadership:
Management should understand the importance of information security and demonstrate leadership by demonstrating its importance to employees. It should clearly define the organization's overall policies and goals regarding information security and communicate them to employees.

Clarifying information Security expectations:
Management should clearly indicate expectations regarding information Security to employees. It is advisable to provide personnel with specific guidance on handling data, managing access rights, adhering to security policies, etc.

Providing education and training:
Regularly implement information security education and training programs within the organization to improve the abilities of personnel. It should provide opportunities for employees to comply with information security policies and understand security best

practices.

Facilitate communication:
Management should communicate important information and changes regarding information Security through communication with employees. Employees should be provided with appropriate channels to submit information security concerns and suggestions.

Feedback and improvements:
Management should accept employee feedback and use it to improve information security processes and policies. It should regularly check the effectiveness of information security through continuous monitoring and evaluation, and make improvements as necessary.

Compliance and rewards:
Management should encourage compliance with information security policies and evaluate employees for practicing appropriate security measures. It should introduce a reward system for good information security practices to increase employee motivation.

C.3. Management Responsibilities
C.3.3.
The management of an Encryption System management organization should develop a mechanism to motivate workers to follow the organization's information security policies.

Guidance
The management of an Encryption System management organization should develop a mechanism to motivate personnel to follow the organization's information security policies. It is recommended that these maintenance methods consider the following:

Clarification of the organization's information security policy:
Management should clearly define the organization's information security policy and communicate it to employees in an easy-to-understand manner. Policies should include specific policies regarding data storage, access control, security protocols, etc.

Promoting education and awareness:
Implement educational programs to regularly emphasize the importance of information

security to personnel and raise their awareness. It should educate employees about the latest security threats and countermeasures through regular training and simulations.

Motivation and rewards:
Introduce an incentive system to encourage personnel to follow information security policies. It should demonstrate rewards for compliance and positive impact on team and individual reputations by reducing security breaches.

Feedback and improvements:
Be open to employee feedback and proactively incorporate issues and suggestions regarding policy implementation. It should identify areas for improvement or ambiguity in policies and make appropriate modifications to improve employee satisfaction and compliance.

Role model suggestions:
It is important for executives and managers to take the initiative in complying with information security policies and to set a good role model for employees. Employees should be influenced positively by leadership and be more likely to follow policies.

Continuous monitoring and improvement:
Continuously monitor compliance with information security policies and detect violations and problems at an early stage. It should improve policies based on monitoring results and improve the security level of the entire organization.

C.3. Managemen**t Responsibilities**

C.3.4.

The management of an Encryption System management organization shall establish a system for workers to achieve a certain level of awareness of information security related to their roles and responsibilities within the organization.

Guidance

The management of an Encryption System management organization shall establish a system for personnel to achieve a certain level of awareness of information security related to their roles and responsibilities within the organization. It is recommended that these maintenance methods consider the following:

Clarification of roles and responsibilities:

Management should clearly define their own roles and responsibilities regarding information security and make them clear to personnel. It should ensure that the roles and responsibilities of each worker are aligned with information security objectives.

Providing education and training:

Implement information security education programs and training within the organization to improve information security knowledge for both management and personnel. It is advisable to provide information security training related to roles and responsibilities and support in achieving certain standards.

Developing regulations and promoting compliance:

Management shall develop information security policies and procedures and promote compliance with them. It is advisable to clearly communicate information security provisions related to their roles and responsibilities to employees and monitor their compliance.

Audit and evaluation:

Regularly audit the implementation status of information security and evaluate the level of compliance. Based on the audit results, it should identify necessary measures and areas for improvement and take appropriate measures.

Transparency and communication:

Management shall ensure transparency regarding information security and promote communication with personnel. It is advisable to provide appropriate information and accept feedback from employees regarding important changes and issues related to information security.

Continuous improvement:

Management shall make continuous efforts to improve information security, and not only maintain certain level, but also constantly aim for improvement. It should periodically re-evaluate and improve information security in order to respond to new threats and technological advances.

C.3. Management Responsibilities

C.3.5.

Management of the Encryption System management organization shall have a system in place to ensure that workers comply with the terms and conditions of employment, including the organization's information security policy and appropriate work practices.

Guidance

Management of the Encryption System management organization shall have a system in place to ensure that personnel comply with the terms and conditions of employment, including the organization's information security policy and appropriate work practices. It is recommended that these maintenance methods consider the following:

Clarification of information security policy:
Management should clearly define the organization's information security policy and require personnel to comply with it. The policy should preferably include specific guidelines regarding data protection, access management, security measures, etc.

Inclusion in terms of employment:
Compliance with information security, including information security policies and appropriate work practices, is incorporated as a condition of employment. Personnel should be required to agree to information security policies when accepting employment contracts and regulations.

Providing education and training:
Provide educational programs and training to personnel regarding information security policies and appropriate work practices. It should provide training on information security basics and policies to new employees and employees in related departments.

Compliance monitoring and evaluation:

Management shall regularly monitor compliance with the information security policy and conduct appropriate evaluations. If a violation or problem occurs, it should take appropriate action and make improvements as necessary.

Rewards and Rewards:
Introduce a system to reward personnel who comply with information security policies and practice appropriate work methods. It should motivate personnel by providing recognition and benefits for good information security practices.

Continuous improvement:
Continuously improve information security policies and appropriate works practices, and strive to improve the organization's security level. It is best to constantly adapt to current conditions by leveraging user feedback and industry best practices.
.

Rewards and Rewards:
A system of rewards and recognition should be introduced for personnel who comply with the information security policy and practice appropriate methods of working, providing certification or benefits for good practice to increase motivation.

Continuous improvement:
Continuously improve information security policies and appropriate work practices, and strive to improve the organization's security level. It is best to constantly adapt to current conditions by leveraging user feedback and industry best practices.

C.3. Management **Responsibilities**

C.3.6.

The management of the Encryption System management organization shall maintain a system for workers to maintain appropriate skills and qualifications and receive regular training.

Guidance

The management of the Encryption System management organization shall maintain a system for personnel to maintain appropriate skills and qualifications and receive regular training. It is recommended that these maintenance methods consider the following:

Clarification of skill and qualification requirements:

Establish clear standards for the skills and qualifications that personnel should have. This preferably includes cryptographic expertise, security management skills, and an understanding of relevant industry regulations and standards.

Educational program design:
Develop regular educational programs. The program aims to provide up-to-date information on new technologies and threats and improve personnel kills. Educational programs should be delivered in a variety of ways, including on-site training, partnerships with external training organizations, and the use of online resources.

Regular evaluation and updates:
Evaluate the effectiveness of educational programs and update as necessary. Programs should be periodically reevaluated and improved to keep pace with technological advances and new threats.

Records management:
Properly manage and track worker education history and credentials. This should ensure that the necessary training is received and qualifications are maintained.

Facilitate communication and feedback:
Promote open communication and gather feedback between personnel and management. It should allow personnel to submit questions and suggestions regarding educational programs and qualification requirements.

C.3. Management **Responsibilities**
C.3.7.
Management of the cryptographic systems management organization should establish mechanisms to provide anonymous reporting channels (e.g., whistleblowing) for workers to report violations of information security policies or procedures.

Guidance
Management of the cryptographic system management organization should establish mechanisms to provide anonymous reporting channels, such as whistleblowing, for personnel to report violations of information Security policies or procedures. It is recommended that these maintenance methods consider the following:

Establishment of anonymous reporting channel:
Management should establish a dedicated reporting channel for anonymously reporting violations of information Security policies and procedures. It is necessary that strict confidentiality and anonymity be ensured through this reporting channel so that personnel can report violations with peace of mind.

Clarification of reporting procedures:
Procedures and methods for anonymous reporting channels should be clearly defined and communicated to personnel. Reporting route information should be posted in appropriate locations within the organization for easy access by personnel.

Protection of reporters:
Take steps to protect the anonymity of posters. Management should take appropriate measures to ensure that posters can report violations without retaliation or disadvantage.

Processing and investigation of reports:
Violation reports posted will be handled appropriately, and prompt and fair investigations will be conducted as necessary. It is essential that responses to violation reports be kept transparent and that interested parties are appropriately notified.

Feedback to reporter:
Providing feedback to anonymous reporters regarding receipt of their report and response status. It should express gratitude to the reporter and demonstrate a positive attitude toward reporting as an organization.

Continuous improvement and transparency:
Continually evaluate and improve the effectiveness and transparency of anonymous reporting channels. It is essential for management to regularly disclose the existence and activities of reporting channels both inside and outside the organization to ensure transparency.
.

C.3. Management Responsibilities

C.3.8.

Management of cryptographic systems management organizations should demonstrate support for and lead by example for information security policies, procedures, and controls.

Guidance

Management of cryptographic systems management organizations should demonstrate support for and lead by example for information security policies, procedures, and controls. These methods of action should consider the following:

Clarification of policies and procedures:

Management shall clearly define policies, procedures, and controls regarding information security and encourage compliance within the organization. Policies and procedures should include specific guidance regarding data storage, access management, information security policy compliance, etc.

Demonstration of support:

Management shall demonstrate support for information security policies and procedures through actions. Management should ensure that policies and procedures are followed through active involvement in information security and the implementation of appropriate measures.

Transparency and communication:

Management should ensure transparency regarding information security policies and procedures and encourage communication with employees. It is advisable to clearly explain the purpose and importance of policies and procedures and to help employees understand their importance and comply with them.

Leadership implications:

Management should demonstrate leadership regarding information security and serve as a positive role model for employees. Management should emphasize its commitment to policies and procedures through regular reporting on information security challenges and successes.

Continuous evaluation and improvement:
Management shall continually evaluate the effectiveness of information security policies and procedures and make improvements as necessary. It is advisable to periodically re-evaluate policies and procedures to keep up with new threats and technological developments, and improve the security level of the organization as a whole.

C.4. Contractor management

C.4.1.

The management of the encrypted system management organization shall confirm through information security policies, procedures, and controls that another organization to which work related to key information and encrypted data and system configuration is outsourced has the following in place for workers.

- **Mechanism to provide guidelines for demonstrating information security expectations in roles within the organization**
- **Mechanism to motivate the organization to follow a set of policies for information security**
- **Mechanism to achieve a certain level of awareness of information security related to one's role and responsibility within the organization**
- **Mechanisms to ensure compliance with terms and conditions of employment, including the organization's information security policy and appropriate work practices**
- **Mechanism to maintain appropriate skills and qualifications and receive regular training**
- **Mechanisms that provide anonymous reporting channels (e.g. whistleblowing) for reporting violations of information security policies or procedures;**

Guidance

The management of the Data Storage System shall establish a mechanism for other organizations to which work related to key information and encrypted data and system configuration are outsourced to provide guidelines to personnel to demonstrate expectations regarding information security. It should consider the following regarding maintenance methods.

Providing guidance:
Ensure that the other organization provides guidance to personnel setting out their roles and

expectations regarding information security. This should ensure that personnel understand their roles and are expected to adhere to appropriate security practices.

Motivation mechanism:
Confirm that a mechanism is in place to motivate other organizations and personnel to comply with information security policies. Ideally, this will include incentive systems, educational programs, and appropriate feedback mechanisms.

Increased awareness:
Confirm that another organization provides mechanisms to improve information security awareness among personnel. It should include training and education programs, evaluation and certification systems, etc.

Compliance with employment conditions:
Ensure that other organizations and personnel have conditions of employment that ensure that they follow information security policies and appropriate work procedures. It is mandatory that this includes contracts, rules, internal regulations, etc.

Education and qualifications provided:
Ensure that other organizations and personnel have appropriate skills and qualifications and provide a mechanism for regular information security training. This encourages personnel to stay informed about the latest security practices and technologies.

Providing anonymous reporting channels:
Verify that another organization provides an anonymous reporting channel for reporting violations of information security policies and procedures. This should make it easier for personnel to report security concerns and issues anonymously.

C.5. Encryption functions provided

C.5.1.

Please specify the following regarding the encryption that can be provided.

• Encryption layer

• Cryptographic algorithm

• How to obtain the key

• Key retention period

• Key protection method

For encryption, use cryptographic algorithms listed in the CRYPTREC list.

Guidance

It should use a cryptographic algorithm listed in the CRYPTREC list for encryption in the data storage area to be encrypted and erased. It should consider the following.

Clear definition of data storage areas:

The organization shall create documented information that clearly defines the data storage areas and scope that will be subject to cryptographic erasure. This documented information should preferably include information such as what data is covered, what format it is stored in, and where it is stored.

Detailed description of target data:

The documented information shall provide a detailed description of the data that will be cryptographically erased. It should include information such as data type, format, retention period, and access privileges.

Explicit range:

The scope of the data storage area is clearly defined and explained in detail in the documented information. It is best to clearly state what is in scope, such as specific servers, databases, file systems, cloud storage, etc.

Clarification of management responsibilities:

The documented information should clearly indicate the management responsibility for the data storage area. It should clearly define who the person in charge or manager is and what kind of authority and responsibility they have.

Update and review process:

The documented information should establish a process for regular updates and reviews. Documented information should be updated and reviewed if necessary, when new data storage areas are added or changes are made.

Access control and monitoring:
Documented information should include policies regarding access control and monitoring of data storage areas. It is imperative that the management of access rights, monitoring of logs, detection of unauthorized access, etc. are clearly defined.

Compliance with legal and regulatory requirements:
Documented information shall be designed to comply with legal and regulatory requirements. Legal and regulatory requirements relating to data storage areas should be included and measures taken to comply should be clearly stated.

C.6. Cryptographic keys are kept only in the Key Management System and not outside the Key Management System.
C.6.1.
Encryption systems should not store cryptographic keys in a non-volatile state.
***If this requirement cannot be met, comply with C.7.7. to C.7.10. as an alternative.**

Guidance
In an Encryption System, it is essential that the cryptographic key is not held in a non-volatile state, and it should consider the following.

Keeping cryptographic keys in a non-volatile state:
In order to avoid holding cryptographic keys in a non-volatile state in order to improve encryption strength and key security, it is necessary that the Data Storage System not hold cryptographic keys in a non-volatile state.

Temporary use of keys:
The cryptographic key is temporarily read into memory and used as needed. After a cryptographic key has been used, it should erase it from memory as soon as possible.

Generate and exchange cryptographic keys:
The cryptographic key is randomly generated using a secure random number generator. The exchange of cryptographic keys is preferably performed via a secure communication path or

key exchange protocol.

Storage of cryptographic keys:
Cryptographic keys are stored using a security mechanism such as a secure Key Management System or hardware security module (HSM). It is essential that cryptographic keys be protected from physical and unauthorized access.

Periodic rotation of cryptographic keys:
Cryptographic keys should be rotated regularly to maintain key strength and security. It is necessary that rotation be performed on a regular schedule based on security policy.

Proper deletion of keys:
Cryptographic keys that are no longer needed should be deleted using an appropriate method. It is necessary that key deletion is important to minimize leakage of confidential information and security risks.

C.7. Access control

C.7.1.

Work with key information and encrypted data, and the assignment of privileges for system configuration, shall be managed through a formal authorization process in accordance with relevant access control policies.

Guidance

For access control, operations related to key information and encrypted data, and assignment of privileges for system configuration should be managed through a formal authorization process in accordance with the relevant access control policy, and the following should be considered.

Compliance with access control policies:
It is mandatory that permissions for operations and system configuration related to key information and encrypted data strictly follow related access control policies.

Formal approval process:
Activities related to key information and encrypted data, as well as changes to system configuration, are managed through a formal authorization process. It is necessary that the

authorization process be approved by an appropriate administrator or responsible person.

Assigning access rights:
Access rights necessary to perform tasks or system configurations related to keying material or encrypted data should be assigned according to the principle of least privilege. It is essential that only the minimum necessary authority be granted, and that the "minimum necessary principle" be followed.

Review and update access rights:
Access rights should be reviewed regularly and updated as necessary. Reviews should be based on changed roles, business requirements, and security risks.

Audit and traceability:
Activities related to key information and encrypted data and changes to system configurations shall be performed in an auditable and traceable manner. All changes should be appropriately logged and audited if necessary.

Education and awareness:
Appropriate training and awareness opportunities will be provided to staff involved in the management of key information and encrypted data. Staff should be educated about the importance of following security and access control policies.

C.7. Access control
C.7.2.
Privileges for working with keys, encrypted data, and configuring systems are assigned based on the minimum requirements of the user's job role.
It is preferable that the account to which system configuration privileges are assigned be linked to an individual user, and that system configuration privileges should not be assigned to an account that is shared by multiple users.

Guidance
Access controls ensure that privileges for working with key information, encrypted data, and system configuration are assigned based on the minimum requirements for the user's job role. It is recommended that the account to which system configuration privileges are assigned be linked to an individual user, and that system configuration privileges should not

be assigned to an account that is shared by multiple users. It should consider the following.

Assign privileges based on minimum requirements:
Privileges for working with key information and encrypted data and configuring systems should be assigned based on the minimum requirements of the user's job role. As a general rule, it should grant users only the necessary privileges and follow the "minimum necessary principle."

Use of personally linked accounts:
The account to which system configuration privileges are assigned shall be an individual account linked to each user. By using accounts linked to individuals, it should track the actions of individual users and clarify where responsibility lies.

Avoiding privilege assignments in shared user accounts:
It is preferable not to assign system configuration privileges to accounts that are shared by multiple users. Shared user accounts make it difficult to manage access and traceability for individual users, so it is recommended to use accounts linked to individuals.

Defining privileges according to role:
Appropriate privileges are defined according to each user's role and responsibility. It is recommended that privileges be reevaluated and adjusted as users' roles and tasks change.

Review and update permissions:
Permissions should be reviewed regularly and updated as necessary. Reviews should be based on changed roles, business requirements, and security risks.

C.7. Access control
C.7.3.
If a user assigned the authority to work on key information, encrypted data, or configure system configuration is replaced due to personnel changes or retirement, access rights shall be changed or deleted.

Guidance
Regarding access control, if a user who has been assigned the authority to work on key

information, encrypted data, or configure system configuration is replaced due to personnel changes or retirement, it should change or delete access rights, and it should consider the following.

Managing access rights due to personnel changes or terminations:
If a user assigned authority to work on key information or encrypted data or to configure system configuration is replaced due to personnel changes or retirement, it should change or delete access rights immediately.

Change steps:
Change or delete access rights by following the prescribed procedures. Change procedures should be in accordance with organizational policies and procedures and should obtain necessary approvals.

Change access rights:
When users change due to personnel changes or retirement, appropriate access rights should be assigned to new users. It should give appropriate privileges to new users according to their roles and responsibilities.

Clear access rights:
Old users' access rights shall be promptly deleted. It is imperative that the deletion procedure be performed in accordance with information Security policy and access control policy.

Ensuring traceability:
The process of changing or erasing access rights shall be appropriately recorded and traceability ensured. It should record information such as the reason for the change, the person who carried out the change, and the date and time of the change.

Audit and review:
The process for changing or erasing access rights shall be regularly audited and reviewed as necessary. Audits and reviews should preferably confirm that changes and deletions of access rights are being implemented appropriately.

C.7. Access control

C.7.4.

Users and systems assigned privileges for working with key information, encrypted data, and system configuration are reviewed at regular intervals.

Guidance

For access control, it should review users and systems assigned privileges for work related to key information and encrypted data, and system configuration at regular intervals, and it should consider the following:

Define review frequency:

Users and systems assigned privileges for working with key information and encrypted data and configuring systems should be reviewed at regular intervals. Review intervals should be defined based on security policy and industry best practices.

Reviewed for:

The review should include all users and systems with authority to work with key information, encrypted data, or configure system configuration. The scope of review should be clearly defined by administrators and security teams.

Review steps:

Reviews should be conducted in accordance with prescribed procedures. Review procedures should include checking access rights, assessing suitability of rights, and detecting unauthorized access.

Assessing the need for change:

If, as a result of the review, changes or updates to access rights are necessary, appropriate procedures will be followed to implement the changes. If changes are required, a formal approval process should be followed before the changes are implemented.

Ensuring traceability:

The review process and results shall be appropriately recorded and traceability shall be ensured. It should record information such as who conducted the review, the results, and why changes were required.

Implementation of improvements:
Appropriate improvement measures shall be implemented based on the results of the review. Remediation measures should be implemented in accordance with security policies and industry best practices.

C.7. Access control
C.7.5.
Records all work with key information, encrypted data, and authorizations assigned to system configuration privileges.

Guidance
For access control, it should record all operations related to key information and encrypted data, as well as all authorizations assigned to system configuration privileges, and it should consider the following:

Authorization record:
When assigning privileges for tasks related to keying information, encrypted data, or system configuration, all authorizations shall be formally recorded. It is necessary that authorization records include information such as who received what authority and the date and time the authority was assigned.

Record contents:
Records should preferably include the following information:
• User or system identifier
• Assigned privileges and roles
• Permission expiration date (if necessary)
• Authority assignment date and time
• Identifier of the administrator who gave the authorization

Storage of information:
Records of approval shall be kept securely. Records should be kept in a location with appropriate access controls in accordance with the highest standards of information Security.

Record tracking:

Approval records shall be maintained appropriately to track change history. When records are changed, the nature and reason for the change should be properly documented information.

Audit and traceability:
Records of authorization shall be subject to periodic audits and security verification. Audits of records should ensure that privilege assignments are properly implemented and comply with security policies.

C.7. Access control
C.7.6.
Do not allow any work with key information, encrypted data, or system configuration until the authorization process is complete.

Guidance
Access control should preferably not allow operations on key information, encrypted data, or system configuration until the authorization process is complete, and the following should be considered:

Prohibited work:
It should prohibit operations related to key information, encrypted data, and system configuration until the authorization process is completed before allowing such operations.

Starting the authorization process:
Before working with key information, encrypted data, or changing system configuration, begin the authorization process. The authorization process should include procedures for obtaining necessary approvals.

Obtaining approval:
Obtain approval from appropriate management and/or interested parties to obtain approvals related to changes to work or system configuration. Approval should preferably be done in a manner that complies with security policies and regulatory requirements.

Process completed:
Perform work or system configuration changes after obtaining necessary approvals. It is

preferable not to permit work until the permitting process is complete and all related procedures and approvals have been established.

Audit and traceability:
Until the approval process is completed, information regarding the process of prohibiting work and obtaining approval should be appropriately recorded and traceability ensured. For audit purposes, it should be able to provide relevant information as needed.

Compliance and education:
Educate all parties on the importance of work prohibitions and approval processes and comply with them. It should promote understanding of how to carry out appropriate procedures through appropriate education and awareness-raising activities.

C.7. Access control

C.7.7.

<Alternative requirements when HYOK cannot be implemented>

Apply controls to prevent anyone from accessing or manipulating key information without authorization or detection.

Specific control measures include monitoring of operation logs, two-person work rules, division of password knowledge, and work after approval by the administrator.

Guidance

Access control is the application of management measures to prevent unauthorized or undetected access or manipulation of key information by a single person. As for specific control measures, it should consider monitoring of operation logs, two-person work rule, division of password knowledge, work after approval by the administrator, etc., and it should consider the following.

Access and operation restrictions:
Even if HYOK cannot be implemented, it should apply control measures to prevent unauthorized or undetected access or manipulation of key information by anyone.

Specific control measures:
The following controls should be considered.
• Monitoring of operation logs: Monitoring of operation logs to detect unauthorized access or

operations when key information is accessed or manipulated.

- Two-person work rule: Important operations and changes to key information shall be performed by two people with the approval and supervision of two or more people.
- Password knowledge division: Dividing the passwords required to access key information among multiple parties and keeping them so that no one can access them alone.
- Work after approval by the administrator: Important operations or changes to key information require approval by the administrator, and the work is executed after approval.

Proper monitoring and traceability:

If alternative requirements are applied, access and operation logs will be appropriately monitored and any unauthorized access or operation will be promptly addressed. It is necessary that logs be stored appropriately and provided for audits and investigations as necessary.

Regular evaluation and improvement:

The effectiveness of alternative requirements shall be periodically evaluated and improved as necessary. Improvements should be made based on security risks and business requirements.

C.7. Access control

C.7.8.

<Alternative requirements when HYOK cannot be implemented>

Separate users who are assigned privileges for working with key information and encrypted data and system configuration, and those who authorize those

Guidance

For access control, it should separate users who are assigned the authority to work on key information and encrypted data and system configuration from those who authorize that authority, and it should consider the following.

Separation of user and authorizer:

It should clearly separate the users who are assigned the authority to work on key information, encrypted data, and system configuration, and the person who authorizes that authority.

Separation of roles and responsibilities:

Clearly define the roles and responsibilities of users and authorizers to avoid confusion. Users perform tasks and operations, and it is essential for an authorizer to play the role of approving those tasks and operations.

Implementation of the approval process:
Implement appropriate authorization processes before assigning new privileges to users. The authorization process should include procedures for obtaining necessary approvals.

Authorization clarification:
When a user obtains a new privilege, the person granting the privilege is clearly identified. Approvers should have appropriate authority and roles and responsibilities that are clearly defined.

Establishment of dual management system:
Establish a dual governance structure to strengthen the separation of users and authorizers. Significant operations and changes should be approved by multiple parties.

Audit and traceability:
Conduct periodic audits to ensure proper separation of users and authorized persons. It is necessary that audit results be appropriately recorded and traceability ensured.

C.7. Access control

C.7.9.

<Alternative requirements when HYOK cannot be implemented>

When users or administrators work on key information or encrypted data or perform system configuration, create control measures to prevent fraud by monitoring activities, audit trails, and supervision by management.

Guidance

For access control, when users or administrators work on key information or encrypted data or perform system configuration, it should develop control measures to prevent fraud by monitoring activities, audit trails, supervision by management, etc., and it should consider the following.

Monitoring activity:

Monitor user or administrator activities in real time as they work on key information, encrypted data, or configure system configuration. It should detect fraud or abnormal activity early through monitoring and take appropriate action.

Creating an audit trail:
Creating an audit trail of logs and events are generated by monitoring activities. It is mandatory that the audit trail includes information such as who did what and when.

Management oversight:
The management layer supervises user activities and administrator actions to prevent fraud. Oversight should preferably include periodic reviews and reports, as well as investigations and responses as necessary.

Rapid response to fraud:
If fraudulent activity is detected through monitoring or analysis of audit trails, respond promptly. It should identify the source of fraud and take appropriate measures to minimize damage.

Training and education:
Provide training and education to users and administrators regarding fraud prevention. It should strive to improve security awareness and disseminate appropriate codes of conduct.

Regular audits and improvements:
Conduct periodic audits and evaluations to confirm the effectiveness of controls. It should improve security levels by improving controls and processes based on audit results.

C.7. Access control
C.7.10.
<Alternative requirements when HYOK cannot be implemented>
Controls to prevent fraud are in place.

Guidance
For access control, it should implement management measures to prevent fraud and it should consider the following.

Operation of controls to prevent fraud:
Confirm that controls to prevent fraud are being operated appropriately. Controls should be developed and implemented based on the organization's security policy and regulatory requirements.

Clarification of control measures:
Controls to prevent fraud should be clearly documented and communicated to interested parties. It is necessary that documented information control measures clearly state the purpose, targets, procedures, and responsible persons.

Definition of operational procedures:
Procedures for operating controls to prevent fraud are clearly defined. The operational procedures should describe who is responsible and what processes and tools will be used to implement them.

Regular evaluation and improvement:
The effectiveness of controls to prevent fraud should be periodically evaluated. It should improve controls and processes as necessary based on the results of the evaluation.

Training and awareness:
Appropriate training and awareness activities are carried out so that interested parties understand how to identify and report fraud. Awareness activities should focus on the latest security threats and best practices.

Reporting and prompt response:
In the event of misconduct, those involved should know the appropriate reporting procedures and be dealt with promptly and appropriately. Processes for reporting and responding to misconduct should be properly documented and communicated.

C.8. Change management

C.8.1.

Change management rules and procedures have been established and approved by the responsible person and those responsible for development and maintenance.

Guidance

For change management, it is essential that change management rules and procedures be established and approved by the person in charge and the person responsible for development and maintenance, and it should consider the following:

Develop change management rules:

Change management rules should comprehensively define procedures for requesting, approving, implementing, monitoring, and evaluating changes. Rules should be developed to align with the organization's vision, goals, and security policies.

Defining change management procedures:

Change management procedures should specifically indicate a series of steps from change request to approval, implementation, and evaluation. The procedures should include those who requests changes, how approval will be obtained, furthermore implementation and testing methods, lastly how future changes will be evaluated.

Appointment of a responsible person:

A responsible person for the change management rules and procedures should be clearly designated. It is mandatory that a responsible person be responsible for each stage of change requests, approval, implementation, monitoring and evaluation.

Approval of development/maintenance manager:

Change control rules and procedures shall be approved by those responsible for development and maintenance. Changes should be made according to approved procedures to ensure consistency and safety.

Documented information changes:

Important decisions and activities at each stage of change management are appropriately documented information. Documented information should include change requests, approvals, implementation procedures, test results, evaluation reports, etc.

Monitoring and evaluation:

Regular monitoring and evaluation should occur even after changes have been implemented. It should appropriately evaluate the impact and outcomes of changes and improve procedures and processes as necessary.

C.8. Change management

C.8.2.

When change management requests occur, the impact on other systems shall be considered.

Guidance

For change management, when a change management request occurs, it should consider the influence of other systems, and it should consider the following.

Evaluation of change requests:

When a change management request occurs, first assess the impact on other systems. In order to accurately understand the scope of impact, it should clearly identify other related systems and services.

Analysis of impact area:

Detailed analysis of the impact of changes on other systems. The scope of impact should preferably include data integrity, system availability, and impact on related processes and workflows.

Collaboration of interested parties:

Work closely with other system owners and interested parties involved in the change management process. It should share information on the scope of impact and change plans, and make necessary agreements and adjustments.

Coordinating change plans:

Adjust change plans appropriately, taking into account the impact on other systems. It should consider the timing and procedures of changes, test plans, etc. so that they are in harmony with other systems.

Implement and monitor changes:

When changes are implemented, monitor the impact on other systems. If the impact of a change is likely to expand unexpectedly, it is advisable to take countermeasures quickly.

Risk management:

Appropriately manage risks related to changes, taking into account the impact on other

systems. It is advisable to consider preventive measures and workarounds to minimize risks and modify change plans as necessary.

C.8. Change management
C.8.3.
Emergency change requests are documented and change control procedures are followed.

Guidance

For change management, urgent change requests should be documented information and change control procedures should be followed, and the following should be considered.

Documented information requirements:
In the event of an emergency change request, the request shall be appropriately documented information. Documented information should include the reason for the change, its scope, impact, and how it will be implemented.

Follow change management procedures:
Emergency change requests should be subject to the same change control procedures as regular changes. Change control procedures should include steps such as request submission, evaluation, approval, implementation, monitoring, and evaluation.

Clarifying priorities:
The priority of urgent change requests is clearly defined. It is essential that priorities be set taking into account the importance, urgency, impact, etc. of changes.

Prompt response:
Urgent change requests shall be responded to promptly. It is necessary that prompt judgment and action be required at each stage of the change management procedure.

Proper documented information:
Even after emergency change requests are approved, they are properly documented information. It is imperative that the details, results, and impacts of implemented changes are appropriately recorded and traceability is ensured.

Monitoring and evaluation:

After emergency changes are implemented, the impact and outcomes of the changes are appropriately monitored and evaluated. If inappropriate changes or impacts occur, it should deal with them promptly.

C.9. System clock

C.9.1.

Prepare a mechanism to ensure the time accuracy of the system clock within the system using time synchronization technology.

Guidance

It should provide a mechanism for ensuring the time accuracy of the system clock within the system using time synchronization technology and it should consider the following.

Selection of time synchronization technology:

Select an appropriate time synchronization technique to ensure the time accuracy of the system clock. It is preferable to use technologies such as NTP (Network Time Protocol) and PTP (Precision Time Protocol).

Setting up a time synchronization server:

Install a time synchronization server in an appropriate location to use time synchronization technology. It is recommended that the server required being highly reliable and easily accessible to the network.

Client configurations:

Clients within each system (servers, workstations, etc.) should be configured to connect to the time synchronization server, periodically obtaining time information from the server to synchronize the system clock.

Security considerations:

Consider the security of time synchronization technology. It should take security measures such as encrypting and authenticating time synchronized communications.

Monitoring and alerts:

Monitor the status of time synchronization and send appropriate alerts if anomalies are detected. It is essential that time synchronization failures and delays be addressed as soon as possible.

Regular evaluation and adjustment:
Perform periodic evaluation and adjustment to maintain accuracy and reliability of time synchronization. It should monitor the time difference between the system clock and the time synchronization server and make adjustments as necessary.

.

C.9. System clock
C.9.2.
The time accuracy of the system clock within the Data Storage System is maintained using time synchronization technology.
Be able to check the time synchronization settings and sampled logs for the above.

Guidance
The system clock shall use time synchronization technology to maintain the time accuracy of the system clock within the Data Storage System. It should be able to check the time synchronization settings and sampled logs, etc., and it should consider the following.

Selection of time synchronization technology:
Select appropriate time synchronization techniques to ensure the time accuracy of system clocks within data storage systems. It should select highly reliable technologies such as NTP (Network Time Protocol) and PTP (Precision Time Protocol).

Build time synchronization settings:
Make appropriate settings to use time synchronization technology. It should ensure that all data storage systems in the system are properly connected to the time synchronization server.

Logging and monitoring:
Recording logs for monitoring time synchronization settings and system clock status. It is necessary that the log includes time synchronization events, system clock change history, and the like.

Regular checks and audits:
Regularly check time synchronization settings and logs to ensure that system clock time accuracy is maintained. It is advisable to conduct an audit to confirm whether the settings

are being implemented appropriately.

Setting up alerts:
If an abnormality or problem with time synchronization is detected, settings should be made so that appropriate alerts are sent. It is imperative that alerts allow problems to be detected and dealt with promptly.

Preparation for troubleshooting steps:
Have appropriate troubleshooting steps in place in case time synchronization issues occur. The procedure should include how to identify the problem and how to resolve it.

D. Key Management System

D. Key Management System

D.1.Security Policy

D.1.1.

The Key Management System management organization shall establish a security policy to protect data. The following shall be clearly stated in the security policy.

a) Appropriate for the purpose of the organization.

b) include information security objectives or provide a framework for setting information security objectives;

c) includes a commitment to meeting applicable requirements related to information security;

d) Access control policy for key information and encrypted data

Guidance

A security policy is an expression of the top-level concept of encryption and erasure as an Encryption System to the outside and inside of an organization. From this perspective, it should formulate a security policy that takes the following into account.

Ensuring suitability:

Security policies should be appropriate to the organization's objectives and consistent with the objectives of the Key Management System.

Clarification of information security objectives:

It is essential that the security policy clearly states the purpose of information security and provides a framework for the Key Management System to protect data and ensure confidentiality and integrity.

Statement of commitment:

The security policy includes an organization-wide commitment to meeting applicable requirements related to information security. Organizations should commit to providing the resources and support necessary to implement and comply with security policies.

Defining access control policy:

It is necessary that the security policy clearly defines access control policies for key information and encrypted data. Access control policies should include authentication,

authorization, and auditing processes, and provide appropriate procedures to maintain confidentiality.

Change management and auditing:
Security policies define change management processes and provide mechanisms for addressing changing security requirements and new threats. Audits and evaluations of policies should be conducted on a regular basis to ensure that policies are being effectively and appropriately implemented.

Education and awareness:
Security policies provide resources and programs to educate and educate interested parties both inside and outside the organization. It is important that all parties involved understand and comply with the security policy, and it should provide appropriate training and information.

D.2. System configuration, and Organizational Structure, roles

D.2.1.

The Key Management System management organization shall prepare documented information that can confirm the roles, responsibilities, and organizational of the organization's own workers who perform work related to key information and encrypted data and system configuration, or of other organizations to which the work is outsourced.

Guidance

System configuration, structure, and role: As a Key Management System management organization, we clarify the system structure, structure, and role in cryptographic erasure. It should clarify the system configuration, structure, and roles in various regulations, organizational charts, etc. From this perspective, it should clarify the system configuration, structure, and roles by considering the following.

Clarification of roles and responsibilities:
The Key Management System management organization shall clearly define the roles and responsibilities of its own personnel who perform work related to key information and encrypted data, as well as the roles and responsibilities of other organizations to which work is outsourced. It should prepare documented information that includes the work content, scope of responsibility, contact information, etc. for each worker or organization.

System development:
The Key Management System management organization will develop an appropriate system for performing work and system configuration related to key information and encrypted data. The structure should include necessary resources, authority, oversight, contact information, etc.

Creating documented information:
Create documented information that confirms the roles, responsibilities, and structure related to work related to key information and encrypted data and system configuration. Documented information should be easy to understand, contain specific information, and be stored in a location that is easily accessible to interested parties.

Regular reviews and updates:
Documented information should be reviewed regularly and updated as necessary. When changes occur to the contents of documented information such as when changes are made or new personnel are added, it should update the documented information promptly.

Notification and Education of Interested parties:
Appropriately notify and explain documented information regarding work and systems related to key information and encrypted data to related parties. It should provide the necessary education and training to ensure that those involved understand their roles and responsibilities and are able to carry out their duties appropriately.

D.2. System configuration, structure, roles
D.2.2.
The Key Management System management organization shall prepare documented information that can confirm the configuration and data flow of the system that handles key information and encrypted data, and its surrounding environment.

Guidance
The Key Management System management organization shall prepare documented information that can confirm the configuration and data flow of the system that handles key information and encrypted data. It should clarify this documented information using a

configuration diagram of the relevant system. From this perspective, it is essential to documented information that the configuration and data flow of the system that handles key information and encrypted data can be confirmed in consideration of the following.

Clarification of system configuration:
The Key Management System management organization clearly documented information the configuration of the system that handles key information and encrypted data. Documented information should preferably include the system's hardware, software, network configuration, etc.

Data flow description:
Describe the data flow related to handling of key information and encrypted data. It is necessary that the procedures and processes from data generation source to storage, processing, transfer, and deletion be clearly described.

Description of security measures:
Documented information should include security measures related to system configuration and data flow. It should include specific measures to strengthen security, such as access control, encryption, and audit log settings.

Description of integration and dependencies between systems:
Clearly explain how the system that handles key information and encrypted data is integrated with other systems, and if there are any dependencies. It should show how to exchange data with other systems and how to share data.

Documented information updates and reviews:
Documented information should be reviewed regularly and updated as necessary. It is necessary that the documented information be updated appropriately when there are changes or upgrades to the system, or the addition of new security requirements.

Sharing and educating interested parties:
Ensure that documented information related to system configuration and data flow are appropriately shared and understood by interested parties. It is advisable to provide appropriate education and training so that interested parties can understand the system configuration and data flow, and understand the importance of security.

D.3. Management Responsibilities

D.3.1.

The management of the Key Management System management organization shall establish a mechanism to appropriately communicate key points regarding information security roles and responsibilities before workers are allowed to work on key information, encrypted data, or access system configuration.

Guidance

The management of the Key Management System management organization shall establish a mechanism to appropriately communicate key points regarding information security roles and responsibilities before personnel are allowed to work on key information, encrypted data, or access system configuration. Possible ways to prepare this information include creating a role/responsibility table. When developing these roles and responsibilities, it should consider the following:

Clarification of management roles and responsibilities:
Management shall understand the importance of information security and recognize its responsibility. It should be responsible for developing and maintaining information security policies.

Education and training for personnel:
Regularly educate and train personnel on the importance and responsibility of information security. It should provide guidelines on how to handle key information and encrypted data and on access privileges to the system.

Dissemination of information security policy:
Disseminate the information security policy within the organization and ensure that all personnel understand and comply with it. If there are any updates or changes to the policy, it is advisable to communicate them appropriately and confirm understanding.

Enhanced access control:
Access to key information and encrypted data should be restricted to the minimum necessary privileges. It is essential that personnel who have been given access authority work only within the scope of their authority.

Audit and evaluation:
Regularly audit information security implementation status and evaluate compliance status. Based on the audit results, it should identify areas for improvement and take appropriate measures.

Risk management and response:
Assess risks related to information security and develop appropriate controls. When a security incident occurs, it should respond promptly and take appropriate measures.

Continuous improvement:
Continually improve information security policies and procedures to keep up with the latest threats and best practices. It should foster a culture in which all members of the organization cooperate in improving information security.

.

D.3. Management Responsibilities

D.3.2.

The management of the Key Management System management organization shall establish a system to provide guidelines to workers to indicate their expectations regarding information security in their roles within the organization.

Guidance

The management of the Key Management System management organization shall establish a system to provide guidelines to personnel to indicate their expectations regarding information Security in their roles within the organization. It is recommended that these maintenance methods consider the following:

Executive leadership:
Management shall understand the importance of information security and demonstrate leadership by demonstrating its importance to employees. It should clearly define the organization's overall policies and goals regarding information security and communicate them to employees.

Clarifying information security expectations:
Management should clearly indicate expectations regarding information security to employees. It is advisable to provide personnel with specific guidance on handling data,

managing access rights, adhering to security policies, etc.

Providing education and training:
Regularly implement information security education and training programs within the organization to improve the abilities of personnel. It should provide opportunities for employees to comply with information security policies and understand security best practices.

Facilitate communication:
Management should communicate important information and changes regarding information security through communication with employees. Employees should be provided with appropriate channels to submit information security concerns and suggestions.

Feedback and improvements:
Management should accept employee feedback and use it to improve information security processes and policies. It should regularly check the effectiveness of information security through continuous monitoring and evaluation, and make improvements as necessary.

Compliance and rewards:
Management should encourage compliance with information security policies and evaluate employees for practicing appropriate security measures. It should introduce a reward system for good information security practices to increase employee motivation.

D.3. Management **Responsibilities**

D.3.3.

The management of the Key Management System management organization should develop a mechanism to motivate workers to follow the organization's information security policies.

Guidance

The management of the Key Management System management organization should develop a mechanism to motivate personnel to follow the organization's information security policies. It is recommended that these maintenance methods consider the following:

Clarification of the organization's information security policy:
Management should clearly define the organization's information Security policy and communicate it to employees in an easy-to-understand manner. Policies should include specific policies regarding data storage, access control, security protocols, etc.

Promoting education and awareness:
Implement educational programs to regularly emphasize the importance of information security to personnel and raise their awareness. It should educate employees about the latest security threats and countermeasures through regular training and simulations.

Motivation and rewards:
Introduce an incentive system to encourage personnel to follow information security policies. It should demonstrate rewards for compliance and positive impact on team and individual reputations by reducing security breaches.

Feedback and improvements:
Be open to employee feedback and proactively incorporate issues and suggestions regarding policy implementation. It should identify areas for improvement or ambiguity in policies and make appropriate modifications to improve employee satisfaction and compliance.

Role model suggestions:
It is important for executives and managers to take the initiative in complying with information security policies and to set a good role model for employees. Employees should be influenced positively by leadership and be more likely to follow policies.

Continuous monitoring and improvement:
Continuously monitor compliance with information security policies and detect violations and problems at an early stage. It should improve policies based on monitoring results and improve the security level of the entire organization.

D.3. Managemen**t Responsibilities**

D.3.4.

The management of the Key Management System management organization shall establish a system for workers to achieve a certain level of awareness of information security related to their roles and responsibilities within the organization.

Guidance

The management of the Key Management System management organization shall establish a system for personnel to achieve a certain level of awareness of information security related to their roles and responsibilities within the organization. It is recommended that these maintenance methods consider the following:

Clarification of roles and responsibilities:

Management should clearly define their own roles and responsibilities regarding information security and make them clear to personnel. It should ensure that the roles and responsibilities of each worker are aligned with information Security objectives.

Providing education and training:

Implement information security education programs and training within the organization to improve information security knowledge for both management and personnel. It is advisable to provide information security training related to roles and responsibilities and support in achieving certain standards.

Developing regulations and promoting compliance:

Management shall develop information security policies and procedures and promote compliance with them. It is advisable to clearly communicate information security provisions related to their roles and responsibilities to employees and monitor their compliance.

Audit and evaluation:

Regularly audit the implementation status of information security and evaluate the level of compliance. Based on the audit results, it should identify necessary measures and areas for improvement and take appropriate measures.

Transparency and communication:

Management shall ensure transparency regarding information security and promote communication with personnel. It is advisable to provide appropriate information and accept feedback from employees regarding important changes and issues related to information security.

Continuous improvement:
Management shall make continuous efforts to improve information security, and not only maintain a certain level, but also constantly aim for improvement. It should periodically re-evaluate and improve information security in order to respond to new threats and technological advances.

D.3. Management **Responsibilities**
D.3.5.
Management of the Key Management System management organization shall have a system in place to ensure that workers comply with the terms and conditions of employment, including the organization's information security policy and appropriate work practices.

Guidance
Management of the Key Management System management organization shall have a system in place to ensure that personnel comply with the terms and conditions of employment, including the organization's information security policy and appropriate work practices. It is recommended that these maintenance methods consider the following:

Clarification of information Security policy:
Management shall clearly define the organization's information Security policy and require personnel to comply with it. The policy should preferably include specific guidelines regarding data protection, access management, security measures, etc.

Inclusion in terms of employment:
Compliance with information security, including information security policies and appropriate work practices, is incorporated as a condition of employment. Personnel should be required to agree to information security policies when accepting employment contracts and regulations.

Providing education and training:
Provide educational programs and training to personnel regarding information security policies and appropriate work practices. It should provide training on information security basics and policies to new employees and employees in related departments.

Compliance monitoring and evaluation:

Management shall regularly monitor compliance with the information security policy and conduct appropriate evaluations. If a violation or problem occurs, it should take appropriate action and make improvements as necessary.

Rewards and Rewards:
Introduce a system to reward personnel who comply with information security policies and practice appropriate work methods. It should motivate personnel by providing recognition and benefits for good information security practices.

Continuous improvement:
Continuously improve information security policies and appropriate work practices, and strive to improve the organization's security level. It is best to constantly adapt to current conditions by leveraging user feedback and industry’s best practices.

D.3. Management Responsibilities
D.3.6.
The management of the Key Management System management organization shall maintain a system for workers to maintain appropriate skills and qualifications and receive regular training.

Guidance
The management of the Key Management System management organization shall maintain a system for personnel to maintain appropriate skills and qualifications and receive regular training. It is recommended that these maintenance methods consider the following:

Clarification of skill and qualification requirements:
Establish clear standards for the skills and qualifications that personnel should have. This preferably includes cryptographic expertise, security management skills, and an understanding of relevant industry regulations and standards.

Educational program design:
Develop regular educational programs. The program aims to provide up-to-date information on new technologies and threats and improve personnel skills. Educational programs should be delivered in a variety of ways, including on-site training, partnerships with external training organizations, and the use of online resources.

Regular evaluation and updates:
Evaluate the effectiveness of educational programs and update as necessary. Programs should be periodically reevaluated and improved to keep pace with technological advances and new threats.

Records management:
Properly manage and track worker education history and credentials. This should ensure that the necessary training is received and qualifications are maintained.

Facilitate communication and feedback:
Promote open communication and gather feedback between personnel and management. It should allow personnel to submit questions and suggestions regarding educational programs and qualification requirements.

D.3. Management Responsibilities
D.3.7.
Management of the Key Management System management organization shall establish mechanisms to provide anonymous reporting channels (e.g., whistleblowing) for workers to report violations of information security policies or procedures.

Guidance
Management of the Key Management System management organization shall establish mechanisms to provide anonymous reporting channels for personnel to report violations of information Security policies or procedures, such as whistleblowing. It is recommended that these maintenance methods consider the following:

Establishment of anonymous reporting channel:
Management should establish a dedicated reporting channel for anonymously reporting violations of information security policies and procedures. It is essential that strict confidentiality and anonymity be ensured through this reporting channel so that personnel can report violations with peace of mind.

Clarification of reporting procedures:
Procedures and methods for anonymous reporting channels should be clearly defined and communicated to personnel. Reporting route information should be posted in appropriate

locations within the organization for easy access by personnel.

Protection of reporters:
Take steps to protect the anonymity of posters. Management should take appropriate measures to ensure that posters can report violations without retaliation or disadvantage.

Processing and investigation of reports:
Violation reports posted will be handled appropriately, and prompt and fair investigations will be conducted as necessary. It is imperative that responses to violation reports be kept transparent and that interested parties be appropriately notified.

Feedback to reporter:
Providing feedback to anonymous reporters regarding receipt of their report and response status. It is necessary to express gratitude to the reporter and to demonstrate a positive attitude toward reporting as an organization.

Continuous improvement and transparency:
Continually evaluate and improve the effectiveness and transparency of anonymous reporting channels. It is mandatory for management to regularly disclose the existence and activities of reporting channels both inside and outside the organization to ensure transparency.

D.3. Management Responsibilities
D.3.8.
The management of the Key Management System management organization shall demonstrate support for the policies, procedures, and controls for information security and act as an example.

Guidance
The management of the Key Management System management organization shall demonstrate support for the policies, procedures, and controls for information Security and act as an example. These methods of action should consider the following:

Clarification of policies and procedures:
Management shall clearly define policies, procedures, and controls regarding information

security and encourage compliance within the organization. Policies and procedures should include specific guidance regarding data storage, access management, security policy compliance, etc.

Demonstration of support:
Management shall demonstrate support for information security policies and procedures through actions. Management should ensure that policies and procedures are followed through active involvement in information Security and the implementation of appropriate measures.

Transparency and communication:
Management should ensure transparency regarding information security policies and procedures and encourage communication with employees. It is advisable to clearly explain the purpose and importance of policies and procedures and to help employees understand their importance and comply with them.

Leadership implications:
Management should demonstrate leadership regarding information security and serve as a positive role model for employees. Management should emphasize its commitment to policies and procedures through regular reporting on information security challenges and successes.

Continuous evaluation and improvement:
Management shall continually evaluate the effectiveness of information security policies and procedures and make improvements as necessary. It is advisable to periodically re-evaluate policies and procedures to keep up with new threats and technological developments, and improve the security level of the organization as a whole.
.

D.4. Contractor management

D.4.1.

The management of the Key Management System management organization shall confirm through information security policies, procedures, and controls that another organization to which work related to key information and encrypted data and system configuration is outsourced has the following in place for workers.

- **Mechanism to provide guidelines for demonstrating information security expectations in roles within the organization**
- **Mechanism to motivate the organization to follow a set of policies for information security**
- **Mechanism to achieve a certain level of awareness of information security related to one's role and responsibility within the organization**
- **Mechanisms to ensure compliance with terms and conditions of employment, including the organization's information security policy and appropriate work practices**
- **Mechanism to maintain appropriate skills and qualifications and receive regular training**
- **Mechanisms that provide anonymous reporting channels (e.g. whistleblowing) for reporting violations of information security policies or procedures;**

Guidance

The management team of the Key Management System management organization should establish a mechanism for other organizations to which work related to key information and encrypted data and system configuration are outsourced to provide guidelines to personnel to demonstrate their expectations regarding information security. It should consider the following regarding maintenance methods.

Providing guidance:

Ensure that the other organization provides guidance to personnel setting out their roles and expectations regarding information security. This should ensure that personnel understand their roles and are expected to adhere to appropriate security practices.

Motivation mechanism:

Confirm that a mechanism is in place to motivate other organizations and personnel to comply with information security policies. Ideally, this will include incentive systems, educational programs, and appropriate feedback mechanisms.

Increased awareness:
Confirm that another organization provides mechanisms to improve information security awareness among personnel. It should include training and education programs, evaluation and certification systems, etc.

Compliance with employment conditions:
Ensure that other organizations and personnel have conditions of employment that ensure that they follow information security policies and appropriate work procedures. It is recommended that this includes contracts, rules, internal regulations, etc.

Education and qualifications provided:
Ensure that other organizations and personnel have appropriate skills and qualifications and provide a mechanism for regular information security training. This encourages personnel to stay informed about the latest security practices and technologies.

Providing anonymous reporting channels:
Verify that another organization provides an anonymous reporting channel for reporting violations of information security policies and procedures. This should make it easier for personnel to report security concerns and issues anonymously.

D.5. Access control

D.5.1.

Work with key information and encrypted data, and the assignment of privileges for system configuration, shall be managed through a formal authorization process in accordance with relevant access control policies.

Guidance

For access control, operations related to key information and encrypted data, and assignment of privileges for system configuration should be managed through a formal authorization process in accordance with the relevant access control policy, and the following should be considered.

Compliance with access control policies:
It is mandatory that permissions for operations and system configuration related to key

information and encrypted data strictly follow related access control policies.

Formal approval process:
Activities related to key information and encrypted data, as well as changes to system configuration, are managed through a formal authorization process. It is essential that the authorization process be approved by an appropriate administrator or responsible person.

Assigning access rights:
Access rights necessary to perform tasks or system configurations related to keying material or encrypted data should be assigned according to the principle of least privilege. It is necessary that only the minimum necessary authority be granted, and that the "minimum necessary principle" be followed.

Review and update access rights:
Access rights should be reviewed regularly and updated as necessary. Reviews should be based on changed roles, business requirements, and security risks.

Audit and traceability:
Activities related to key information and encrypted data and changes to system configurations shall be performed in an auditable and traceable manner. All changes should be appropriately logged and audited if necessary.

Education and awareness:
Appropriate training and awareness opportunities will be provided to staff involved in the management of key information and encrypted data. Staff should be educated about the importance of following security and access control policies.

D.5. Access control
D.5.2.
Privileges for working with keys, encrypted data, and configuring systems are assigned based on the minimum requirements of the user's job role.
It is preferable that the account to which system configuration privileges are assigned be linked to an individual user, and that system configuration privileges should not be assigned to an account that is shared by multiple users.

Guidance

Access controls ensure that privileges for working with key information, encrypted data, and system configuration are assigned based on the minimum requirements for the user's job role. It is recommended that the account to which system configuration privileges are assigned be linked to an individual user, and that system configuration privileges should not be assigned to an account that is shared by multiple users. It should consider the following.

Assign privileges based on minimum requirements:

Privileges for working with key information and encrypted data and configuring systems should be assigned based on the minimum requirements of the user's job role. As a general rule, it should grant users only the necessary privileges and follow the "minimum necessary principle."

Use of personally linked accounts:

The account to which system configuration privileges are assigned shall be an individual account linked to each user. By using accounts linked to individuals, it should track the actions of individual users and clarify where responsibility lies.

Avoiding privilege assignments in shared user accounts:

It is preferable not to assign system configuration privileges to accounts that are shared by multiple users. Shared user accounts make it difficult to manage access and traceability for individual users, so it is recommended to use accounts linked to individuals.

Defining privileges according to role:

Appropriate privileges are defined according to each user's role and responsibility. It is recommended that privileges be reevaluated and adjusted as users' roles and tasks change.

Review and update permissions:

Permissions should be reviewed regularly and updated as necessary. Reviews should be based on changed roles, business requirements, and security risks.

D.5. Access control

D.5.3.

If a user assigned the authority to work on key information, encrypted data, or configure system configuration is replaced due to personnel changes or retirement, access rights shall be changed or deleted.

Guidance

Regarding access control, if a user who has been assigned the authority to work on key information, encrypted data, or configure system configuration is replaced due to personnel changes or retirement, it should change or delete access rights, and it should consider the following.

Managing access rights due to personnel changes or terminations:

If a user assigned authority to work on key information or encrypted data or to configure system configuration is replaced due to personnel changes or retirement, it should change or delete access rights immediately.

Change steps:

Change or delete access rights by following the prescribed procedures. Change procedures should be in accordance with organizational policies and procedures and should obtain necessary approvals.

Change access rights:

When users change due to personnel changes or retirement, appropriate access rights should be assigned to new users. It should give appropriate privileges to new users according to their roles and responsibilities.

Clear access rights:

Old users' access rights shall be promptly deleted. It is necessary that the deletion procedure be performed in accordance with information security policy and access control policy.

Ensuring traceability:

The process of changing or erasing access rights shall be appropriately recorded and traceability ensured. It should record information such as the reason for the change, the person who carried out the change, and the date and time of the change.

Audit and review:

The process for changing or erasing access rights shall be regularly audited and reviewed as necessary. Audits and reviews should preferably confirm that changes and deletions of access rights are being implemented appropriately.

D.5. Access control

D.5.4.

Users and systems assigned privileges for working with key information, encrypted data, and system configuration are reviewed at regular intervals.

Guidance

For access control, it should review users and systems assigned privileges for work related to key information and encrypted data, and system configuration at regular intervals, and it should consider the following:

Define review frequency:

Users and systems assigned privileges for working with key information and encrypted data and configuring systems should be reviewed at regular intervals. Review intervals should be defined based on security policy and industry best practices.

Reviewed for:

The review should include all users and systems with authority to work with key information, encrypted data, or configure system configuration. The scope of review should be clearly defined by administrators and security teams.

Review steps:

Reviews should be conducted in accordance with prescribed procedures. Review procedures should include checking access rights, assessing suitability of rights, and detecting unauthorized access.

Assessing the need for change:

If, as a result of the review, changes or updates to access rights are necessary, appropriate procedures will be followed to implement the changes. If changes are required, a formal approval process should be followed before the changes are implemented.

Ensuring traceability:

The review process and results shall be appropriately recorded and traceability shall be ensured. It should record information such as who conducted the review, the results, and why changes were required.

Implementation of improvements:

Appropriate improvement measures shall be implemented based on the results of the review. Remediation measures should be implemented in accordance with security policies and industry best practices.

D.5. Access control

D.5.5.

Records all work with key information, encrypted data, and authorizations assigned to system configuration privileges.

Guidance

For access control, it should record all operations related to key information and encrypted data, as well as all authorizations assigned to system configuration privileges, and it should consider the following:

Authorization record:

When assigning privileges for tasks related to keying information, encrypted data, or system configuration, all authorizations shall be formally recorded. It is necessary that authorization records include information such as who received what authority and the date and time the authority was assigned.

Record contents:

Records should preferably include the following information:

• User or system identifier
• Assigned privileges and roles
• Permission expiration date (if necessary)
• Authority assignment date and time
• Identifier of the administrator who gave the authorization

Storage of information:

Records of approval shall be kept securely. Records should be kept in a location with appropriate access controls in accordance with the highest standards of information security.

Record tracking:

Approval records shall be maintained appropriately to track change history. When records

are changed, the nature and reason for the change should be properly documented information.

Audit and traceability:
Records of authorization shall be subject to periodic audits and security verification. Audits of records should ensure that privilege assignments are properly implemented and comply with security policies.

D.5. Access control
D.5.6.
Do not allow any work with key information, encrypted data, or system configuration until the authorization process is complete.

Guidance
Access control should preferably not allow operations on key information, encrypted data, or system configuration until the authorization process is complete, and the following should be considered:

Prohibited work:
It should prohibit operations related to key information, encrypted data, and system configuration until the authorization process is completed before allowing such operations.

Starting the authorization process:
Before working with key information, encrypted data, or changing system configuration, begin the authorization process. The authorization process should include procedures for obtaining necessary approvals.

Obtaining approval:
Obtain approval from appropriate management and/or interested parties to obtain approvals related to changes to work or system configuration. Approval should preferably be done in a manner that complies with security policies and regulatory requirements.

Process completed:
Perform work or system configuration changes after obtaining necessary approvals. It is preferable not to permit work until the permitting process is complete and all related

procedures and approvals have been established.

Audit and traceability:
Until the approval process is completed, information regarding the process of prohibiting work and obtaining approval should be appropriately recorded and traceability ensured. For audit purposes, it should be able to provide relevant information as needed.

Compliance and education:
Educate all parties on the importance of work prohibitions and approval processes and comply with them. It should promote understanding of how to carry out appropriate procedures through appropriate education and awareness-raising activities.

D.5. Access control

D.5.7.

Apply controls to prevent anyone from accessing or manipulating key information without authorization or detection.

Specific control measures include monitoring of operation logs, two-person work rules, division of password knowledge, and work after approval by the administrator.

Guidance

Access control is the application of management measures to prevent unauthorized or undetected access or manipulation of key information by a single person. As for specific control measures, it should consider monitoring of operation logs, two-person work rule, division of password knowledge, work after approval by the administrator, etc., and it should consider the following.

Access and operation restrictions:
It should apply control measures to prevent anyone from accessing or manipulating key information without authorization or detection.

Specific control measures:
The following controls should be considered.

- Monitoring of operation logs: Monitoring of operation logs to detect unauthorized access or operations when key information is accessed or manipulated.
- Two-person work rule: Important operations and changes to key information shall be

performed by two people with the approval and supervision of two or more people.

- Password knowledge division: Dividing the passwords required to access key information among multiple parties and keeping them so that no one can access them alone.
- Work after approval by the administrator: Important operations or changes to key information require approval by the administrator, and the work is executed after approval.

Proper monitoring and traceability:
If alternative requirements are applied, access and operation logs will be appropriately monitored and any unauthorized access or operation will be promptly addressed. It is necessary that logs be stored appropriately and provided for audits and investigations as necessary.

Regular evaluation and improvement:
The effectiveness of alternative requirements shall be periodically evaluated and improved as necessary. Improvements should be made based on security risks and business requirements.

D.5. Access control
D.5.8.
Separate users who are assigned privileges for working with key information and encrypted data and system configuration, and those who authorize those

Guidance
For access control, it should separate users who are assigned the authority to work on key information and encrypted data and system configuration from those who authorize that authority, and it should consider the following.

Separation of user and authorizer:
It should clearly separate the users who are assigned the authority to work on key information, encrypted data, and system configuration, and the person who authorizes that authority.

Separation of roles and responsibilities:
Clearly define the roles and responsibilities of users and authorizers to avoid confusion.

Users perform tasks and operations, and it is essential for an authorizer to play the role of approving those tasks and operations.

Implementation of the approval process:
Implement appropriate authorization processes before assigning new privileges to users. The authorization process should include procedures for obtaining necessary approvals.

Authorization clarification:
When a user obtains a new privilege, the person granting the privilege is clearly identified. Approvers should have appropriate authority and roles and responsibilities that are clearly defined.

Establishment of dual management system:
Establish a dual governance structure to strengthen the separation of users and authorizers. Significant operations and changes should be approved by multiple parties.

Audit and traceability:
Conduct periodic audits to ensure proper separation of users and authorized persons. It is mandatory that audit results be appropriately recorded and traceability ensured.

D.5. Access control

D.5.9.

When users or administrators work on key information or encrypted data or perform system configuration, create control measures to prevent fraud by monitoring activities, audit trails, and supervision by management.

Guidance

For access control, when users or administrators work on key information or encrypted data or perform system configuration, it should develop control measures to prevent fraud by monitoring activities, audit trails, supervision by management, etc., and it should consider the following.

Monitoring activity:
Monitor user or administrator activities in real time as they work on key information, encrypted data, or configure system configuration. It should detect fraud or abnormal activity early

through monitoring and take appropriate action.

Creating an audit trail:
Creating an audit trail of logs and events generated by monitoring activities. It is necessary that the audit trail includes information such as who did what and when.

Management oversight:
The management layer supervises user activities and administrator actions to prevent fraud. Oversight should preferably include periodic reviews and reports, as well as investigations and responses as necessary.

Rapid response to fraud:
If fraudulent activity is detected through monitoring or analysis of audit trails, respond promptly. It should identify the source of fraud and take appropriate measures to minimize damage.

Training and education:
Provide training and education to users and administrators regarding fraud prevention. It should strive to improve security awareness and disseminate appropriate codes of conduct.

Regular audits and improvements:
Conduct periodic audits and evaluations to confirm the effectiveness of controls. It should improve security levels by improving controls and processes based on audit results.

D.5. Access control
D.5.10.
Controls to prevent fraud are in place.

Guidance
For access control, it should implement management measures to prevent fraud, and it should consider the following.

Operation of controls to prevent fraud:
Confirm that controls to prevent fraud are being operated appropriately. Controls should be

developed and implemented based on the organization's security policy and regulatory requirements.

Clarification of control measures:
Controls to prevent fraud should be clearly documented information and communicated to interested parties. It is imperative that documented information control measures clearly state the purpose, targets, procedures, and responsible person.

Definition of operational procedures:
Procedures for operating controls to prevent fraud are clearly defined. The operational procedures should describe who is responsible and what processes and tools will be used to implement them.

Regular evaluation and improvement:
The effectiveness of controls to prevent fraud should be periodically evaluated. It should improve controls and processes as necessary based on the results of the evaluation.

Training and awareness:
Appropriate training and awareness activities are carried out so that interested parties understand how to identify and report fraud. Awareness activities should focus on the latest security threats and best practices.

Reporting and prompt response:
In the event of misconduct, those involved should know the appropriate reporting procedures and be dealt with promptly and appropriately. Processes for reporting and responding to misconduct should be properly documented and communicated.

D.6.Key lifecycle management
D.6.1.
Use FIPS140-2 or FIPS140-3 Level 1 compliant products for key storage.

Guidance
For key lifecycle management, it should use a FIPS140-2 or FIPS140-3 level 1 compliant product for key storage, and it should consider the following:

Ensure FIPS140-2 or FIPS140-3 Level 1 compliance:
For key storage, it should ensure level 1 compliance based on FIPS140-2 or FIPS140-3 standards to ensure key security and meet regulatory requirements.

Choosing the right Key Management System:
Implement an appropriate Key Management System using FIPS140-2 or FIPS140-3 compliant products. This should include procedures for key generation, storage, distribution, and deletion.

Ensuring safe storage of keys:
Select the physical location and digital environment where keys will be stored and implement appropriate security measures. This should include access control, monitoring, logging, and establishing appropriate backup procedures.

Regular audits and evaluations:
Regularly audit key storage processes to ensure compliance with security policies and regulatory requirements. It also should evaluate the performance and security of the Key Management System and make improvements as necessary.

Ongoing training and education:
Provide key management personnel with appropriate training and education to understand best practices based on FIPS standards. It is hoped that this will ensure proper key storage and security.

D.6.Key lifecycle management
D.6.2.
When the Data Owner organization requests presentation of the key generation log, the generation log shall be presented to the Data Owner organization.

Guidance
When the Data Owner organization requests presentation of the key generation log, it should present the generation log to the Data Owner organization, and it should consider the following.

Reception and evaluation of requests:
When we receive a request to present a key generation log from a Data Owner organization, we immediately accept the request and evaluate the request. It is advisable to check the validity of the request and request additional information if necessary.

Extract and serve appropriate logs:
If key generation logs are required, extract the logs based on appropriate procedures and provide them to the Data Owner organization. It is imperative that logs be provided in a safe and appropriate manner.

Protecting confidential information:
Key generation logs may contain confidential information so when providing logs, take appropriate security measures to minimize the risk of information leakage. This should include encrypting logs, selecting secure transmission methods, and implementing access controls.

Documented information and record requests:
Appropriately documented information and maintain records of responses to requests for key generation logs from Data Owner organizations. This preferably includes information such as the content of the request, details of the logs provided, and the date and time of the response.

Appropriate communication and feedback:
Ensure communication with the Data Owner organization and ensure that requests are appropriately addressed. It also should collect feedback on the provided logs and make appropriate improvements as necessary.

D.6.Key lifecycle management
D.6.3.
When the Data Owner organization requests the destruction of the key, after destroying the key, present the destruction log to the Data Owner organization.

Guidance
When a Data Owner organization requests the destruction of a key, it should present a destruction log to the Data Owner organization after the key is destroyed, and it should

consider the following.

Reception and evaluation of requests:
When receiving a request for key destruction from a Data Owner organization, immediately accept the request and evaluate the request. It is advisable to check the validity of the request and request additional information if necessary.

Implement proper disposal procedures:
If a key destruction request is approved, appropriate destruction procedures shall be implemented. This includes removing, destroying, or otherwise disposing of keys. Appropriate procedures and standards should be followed when disposing of keys to minimize security risks.

Creating a disposal log:
After key destruction is complete, create a destruction log. This log preferably includes identification information of the revoked key, date and time of revocation, and details of the revocation procedure.

Log provided:
Once the disposal log is created, present the log to the Data Owner organization. It is essential that logs be provided in a safe and appropriate manner.

Protecting confidential information:
Disposal logs may contain confidential information so when providing logs, take appropriate security measures to minimize the risk of information leakage. This should include encrypting logs, selecting secure transmission methods, and implementing access controls.

Documented information and record requests:
Appropriately documented information and maintain records of responses to key destruction requests from Data Owner organizations. This preferably includes information such as the content of the request, details of the logs provided, and the date and time of the response.

Appropriate communication and feedback:
Ensure communication with the Data Owner organization and ensure that requests are appropriately addressed. It should collect feedback on the provided logs and make

appropriate improvements as necessary.

D.6.Key lifecycle management

D.6.4.

When key information is taken out of a Key Management System, prevent the key from being restored using the key information taken out of the Key Management System.

Guidance

If key information is taken outside the Key Management System, it should prevent the key from being restored using the key information taken outside the Key Management System, and it should consider the following.

Restrictions and management of external exports:

In principle, key information should be kept within the Key Management System, but if it is necessary to take it outside under certain circumstances, it is necessary to obtain permission from the administrator in advance. It is necessary that permission for external use be approved by an administrator with appropriate authority and recorded.

Clarification of purpose and period of export:

The purpose and period of export shall be clearly defined. This should preferably include valid reasons such as external work or participation in a specific project.

Implementation of security measures when taking out:

Appropriate security measures shall be taken when key information is taken outside. This should include encrypting key information, using secure data transfer methods, and implementing access controls.

Permission to temporarily use key information:

When key information taken outside is used temporarily, it is necessary to automatically invalidate the key information after the usage period ends. This can be expected to minimize the risk of unauthorized use or leakage of key information.

Securing unrecoverable key information:

Appropriate technical measures shall be implemented to ensure that keys cannot be recovered using key information taken externally. This preferably includes temporary

changes to key information and automatic invalidation of key information once used.

Monitoring and logging:
Monitor the use of key information taken outside and record logs if necessary. As a result, a quick response can be expected in the event of unauthorized use or leakage of key information.

D.6.Key lifecycle management
D.6.5.
If key information is taken out of the Key Management System, the policy should clearly state that after the key is discarded in the Key Management System, the key information that was taken out will also be discarded and restoring the key from the key information will be prohibited.

Guidance
If key information is taken out of the Key Management System, it should clearly state in the policy that after the key is discarded in the Key Management System, the key information that has been taken out is also discarded and restoration of the key from the key information is prohibited, and it should consider the following.

Restrictions and management of external exports:
In principle, key information should be kept within the Key Management System, but taking it outside should be limited to the minimum necessary. It is preferable that permission to take items outside is approved by an administrator with appropriate authority, and that the purpose and period are clearly defined.

Disposal of key information after disposal:
After the key is discarded in the Key Management System, the key information taken outside should be discarded as well. It is expected that this will prohibit key recovery from key information taken outside.

Disposal policy stated:
The policy documented information for the Key Management System should clearly state the policy regarding the removal of key information specifically, after the key is discarded in the Key Management System, it should discard the key information taken out and prohibit

recovery of the key from the key information.

Improving security awareness:
It is important to educate users of key management systems and related parties about the risks of taking keys outside and the importance of policies. It is essential that increased security awareness promotes policy compliance.

Monitoring and auditing:
Activities related to key removal and disposal should be monitored and regular audits performed. Through this, it should confirm the compliance status of the policy and take remedial measures as necessary.

D.6.Key lifecycle management
D.6.6.
If key information (keys and key metadata) is to be transferred outside the Key Management System, it shall be delivered in a secure manner as defined by industry best practices and guidelines.

Guidance
If key information (keys and key metadata) is to be exported outside the Key Management System, it is preferable to do so in a secure manner as defined by industry best practices and guidelines, and the following should be considered:

Purpose and permission for removal:
If it becomes necessary to take out key information, it is necessary to clarify the purpose and obtain permission from an administrator with appropriate authority. It should properly document the purpose and period of removal and establish an approval process.

Compliance with industry best practices and guidelines:
Adhere to industry best practices and guidelines regarding key exfiltration. It is advisable to refer to security guidelines and best practices provided by industry associations and regulatory bodies.

Choose a safe shipping method:
Choose industry-standard secure methods to securely deliver key information. This preferably includes the use of encrypted communication channels, the use of secure data

transfer protocols, and the use of reliable carriers.

Data encryption:
Encrypt data as necessary before taking key information outside. This is expected to protect data from unauthorized access and ensure confidentiality.

Access control when sending:
When transmitting key information externally, strictly limit the destination and limit the people who can access the transmitted information. This is expected to minimize the risk of information leakage and unauthorized use.

Monitoring and tracing during transmission:
Monitoring the key information transmission process to ensure that the transmitted information reaches the appropriate recipient. It should record a log at the time of transmission and retain traceable information.

D.7. Change management

D.7.1.

Change management rules and procedures have been established and approved by the responsible person and those responsible for development and maintenance.

Guidance

For change management, it is imperative that change control rules and procedures be established and approved by the person in charge and the person responsible for development and maintenance, and it should consider the following:

Develop change management rules:
Change management rules should comprehensively define procedures for requesting, approving, implementing, monitoring, and evaluating changes. Rules should be developed to align with the organization's vision, goals, and security policies.

Defining change control procedures:
Change management procedures should specifically indicate a series of steps from change

request to approval, implementation, and evaluation. The procedures should include who requests changes, how approval will be obtained, implementation and testing methods, and how changes will be evaluated.

Appointment of responsible person:
Persons responsible for change control rules and procedures should be clearly designated. It is necessary that a responsible person be responsible for each stage of change requests, approval, implementation, monitoring, and evaluation.

Approval of development/maintenance manager:
Change control rules and procedures shall be approved by those responsible for development and maintenance. Changes should be made according to approved procedures to ensure consistency and safety.

Documented information changes:
Important decisions and activities at each stage of change management are appropriately documented information. Documented information should include change requests, approvals, implementation procedures, test results, evaluation reports, etc.

Monitoring and evaluation:
Regular monitoring and evaluation should occur even after changes have been implemented. It should appropriately evaluate the impact and outcomes of changes and improve procedures and processes as necessary.

D.7. Change management
D.7.2.
When change management requests occur, the impact on other systems shall be considered.

Guidance
For change management, when a change management request occurs, it should consider the influence of other systems, and it should consider the following.

Evaluation of change requests:
When a change management request occurs, first assess the impact on other systems. In order to accurately understand the scope of impact, it should clearly identify other related

systems and services.

Analysis of impact area:
Detailed analysis of the impact of changes on other systems. The scope of impact should preferably include data integrity, system availability, and impact on related processes and workflows.

Collaboration of interested parties:
Work closely with other system owners and interested parties involved in the change management process. It should share information on the scope of impact and change plans, and make necessary agreements and adjustments.

Coordinating change plans:
Adjust change plans appropriately, taking into account the impact on other systems. It should consider the timing and procedures of changes, test plans, etc. so that they are in harmony with other systems.

Implement and monitor changes:
When changes are implemented, monitor the impact on other systems. If the impact of a change is likely to expand unexpectedly, it is advisable to take countermeasures quickly.

Risk management:
Appropriately manage risks related to changes, taking into account the impact on other systems. It is advisable to consider preventive measures and workarounds to minimize risks and modify change plans as necessary.

D.7. Change management
D.7.3.
Emergency change requests are documented and change control procedures are followed.

Guidance

For change management, urgent change requests should be documented and change control procedures should be followed, and the following should be considered.

Documented information requirements:
In the event of an emergency change request, the request shall be appropriately documented

information. Documented information should include the reason for the change, its scope, impact, and how it will be implemented.

Follow change control procedures:
Emergency change requests should be subject to the same change control procedures as regular changes. Change control procedures should include steps such as request submission, evaluation, approval, implementation, monitoring, and evaluation.

Clarifying priorities:
The priority of urgent change requests is clearly defined. It is necessary that priorities be set taking into account the importance, urgency, impact, etc. of changes.

Prompt response:
Urgent change requests shall be responded to promptly. It is essential that prompt judgment and action be required at each stage of the change control procedure.

Proper documented information:
Even after emergency change requests are approved, they are properly documented. It is mandatory that the details, results, and impacts of implemented changes are appropriately recorded and traceability is ensured.

Monitoring and evaluation:
After emergency changes are implemented, the impact and outcomes of the changes are appropriately monitored and evaluated. If inappropriate changes or impacts occur, it should deal with them promptly.

D.8. System clock

D.8.1.

Prepare a mechanism to ensure the time accuracy of the system clock within the system using time synchronization technology.

Guidance

It should provide a mechanism for ensuring the time accuracy of the system clock within the system using time synchronization technology, and it should consider the following.

Selection of time synchronization technology:
Select an appropriate time synchronization technique to ensure the time accuracy of the system clock. It is preferable to use technologies such as NTP (Network Time Protocol) and PTP (Precision Time Protocol).

Setting up a time synchronization server:
Install a time synchronization server in an appropriate location to use time synchronization technology. It is necessary that the server be highly reliable and easily accessible to the network.

Client settings:
Setting up a connection to a time synchronization server for clients (servers, workstations, etc.) in each system. It is essential that the client periodically obtains time information from the time synchronization server and synchronizes the system clock.

Security considerations:
Consider the security of time synchronization technology. It should take security measures such as encrypting and authenticating time synchronized communications.

Monitoring and alerts:
Monitor the status of time synchronization and send appropriate alerts if anomalies are detected. It is essential that time synchronization failures and delays be addressed as soon as possible.

Regular evaluation and adjustment:
Perform periodic evaluation and adjustment to maintain accuracy and reliability of time synchronization. It should monitor the time difference between the system clock and the time synchronization server and make adjustments as necessary.

D.8. System clock
D.8.2.
The time accuracy of the system clock within the Data Storage System is maintained using time synchronization technology.
Be able to check the time synchronization settings and sampled logs for the above.

Guidance

The system clock shall use time synchronization technology to maintain the time accuracy of the system clock within the Data Storage System. It should be able to check the time synchronization settings and sampled logs, etc., and it should consider the following.

Selection of time synchronization technology:

Selecting appropriate time synchronization techniques to ensure the time accuracy of system clocks within data storage systems. It should select highly reliable technologies such as NTP (Network Time Protocol) and PTP (Precision Time Protocol).

Build time synchronization settings:

Make appropriate settings to use time synchronization technology. It should ensure that all data storage systems in the system are properly connected to the time synchronization server.

Logging and monitoring:

Recording logs for monitoring time synchronization settings and system clock status. It is necessary that the log includes time synchronization events, system clock change history, and the like.

Regular checks and audits:

Regularly check time synchronization settings and logs to ensure that system clock time accuracy is maintained. It is advisable to conduct an audit to confirm whether the settings are being implemented appropriately.

Setting up alerts:

If an abnormality or problem with time synchronization is detected, settings should be made so that appropriate alerts are sent. It is essential that alerts allow problems to be detected and dealt with promptly.

Preparation for troubleshooting steps:

Have appropriate troubleshooting steps in place in case time synchronization issues occur. The procedure should include how to identify the problem and how to resolve it.

Council for Proper Data Erasure Execution Certification
CSP Certification Standards WG members

Leader: Tatsuro Saisho (Sakura Internet Co., Ltd.) [Chairman of the Management Executive Committee]
Members: Daisuke Yoshikawa (Canon IT Solutions Inc.)
: Junichi Okabe (ISACA Tokyo Chapter Vice President and Director)
: Teruaki Murakami (P Mark Lead Auditor /ISMS Assistant Auditor)
: Tetsuya Sakamoto (Ultra X Co., Ltd.)
: Osamu Numata (Digital Forensics Study Group) [Technical Advisor]
: Akira Otaishi (PPAP Souken LLC)
: Hiroshi Itani (NetApp LLC)
: Takeshi Kanzawa (NetApp LLC)
Observer: Tetsutaro Uehara (Professor, College of Information Science and Technology, Ritsumeikan University)
: Masato Kanda (Independent Administrative Agency Information-technology Promotion Agency)

Publisher: Data Deletion Execution Certification Council CSP Certification Standards WG member
Publication date: December 17, 2024