Information Security Policy

Osotspa Public Company Limited and its affiliates

Effective from May 1, 2025 onwards

Enforced from May 1, 2025 onwards

Document Control

Approved by (Wannipa Bhakdibutr) Chief Executive Officer	
Reviewed by (Pajaree Saengcum) Head of Digital Technology	**Prepared by** (Anupas Siriwej) Head of Digital Service Excellence

OSOTSPA	**Unit / Division :** Digital Technology	
	Document Type : Policy	
	Document Number : M-HM-ITD-001	**Revision : 4**
	Effective Date : May 1, 2025	**Page No. : 2** of **29**

Subject : Information Security Policy

Revision History

Last reviewed : April 2025

Next review : April 2026

Revision No.	Effective Date	Revision Details
00	13 May 2016	Initial Version
01	1 March 2020	- Revision of the Thai policy title - Comprehensive content update
02	1 January 2024	- Revision of retention period - Amendment of department name
03	1 April 2024	- Revision of English policy title
04	1 May 2025	- Add section on Data Security - Revise content on Cryptographic Control - Adjust frequency of penetration testing

OSOTSPA	**Unit / Division :** Digital Technology	
	Document Type : Policy	
	Document Number : M-HM-ITD-001	**Revision :** **4**
	Effective Date : May 1, 2025	**Page No. :** **3** of **29**

Subject : Information Security Policy

InformationSecurity Policy

OSOTSPA	**Unit / Division :** Digital Technology	
	Document Type : Policy	
	Document Number : M-HM-ITD-001	**Revision :** 4
	Effective Date : May 1, 2025	**Page No. :** 4 of 29

Subject : Information Security Policy

Introduction

Osotspa Public Company Limited has established this Information Security Policy to govern and manage information technology and ensure the security of information systems. The policy requires the implementation of controls, monitoring, and audits to ensure compliance, prevent IT-related risks, and ensure that computer systems and networks operate efficiently and effectively, supporting the business operations of Osotspa Public Company Limited and its affiliates, both domestically and internationally.

This policy sets a uniform standard that all employees and users are required to follow.

Objective

1. To establish standards, guidelines, and procedures for the secure use of information systems by users, ensuring operations are efficient, effective, and aligned with defined objectives, while raising user awareness of the importance of information technology security.
2. To prevent information systems and data from unauthorized access, attacks, alteration, destruction, or any actions that may cause damage to business operations.
3. To set standards and practices for managing information systems and data in compliance with relevant laws and regulations, including personal data protection laws.
4. To communicate the policy to users and authorized external parties who have access to information or information systems, ensuring they acknowledge and strictly adhere to it.

Scope of Responsibilities

Osotspa Public Company Limited has established a written Information Security Policy, which shall be reviewed or updated by the Digital Technology Department at least once a year or whenever changes occur in the environment, such as business conditions, regulations, laws, or technology.

The policy shall be made accessible to users so that employees and relevant users are informed and comply with its provisions. All employees and users are required to learn, understand, and strictly follow the Information Security Policy, fully cooperate in protecting computer systems and information, and continuously monitor, supervise, and safeguard information and information systems to ensure their security.

Penalties

This Information Security Policy is an integral part of the work requirements for all employees and users.

Any individual found violating or failing to comply with the policy may be subject to disciplinary action in accordance with the regulations of Osotspa Public Company Limited, and legal proceedings may be pursued if the violation constitutes an offense under the applicable Computer Crime Act and other relevant laws in force at that time.

OSOTSPA	**Unit / Division :** Digital Technology	
	Document Type : Policy	
	Document Number : M-HM-ITD-001	**Revision :** 4
	Effective Date : May 1, 2025	**Page No. :** 5 of 29

Subject : Information Security Policy

Section 1 : Governance of Enterprise IT

Introduction

Currently, information technology systems play a crucial role in driving business operations and are considered one of the core systems any disruption may impact business continuity.

Therefore, senior management must play a key role in managing and implementing information technology systems to support business activities. They are also responsible for translating corporate mission, strategy, policies, and organizational plans into objectives related to information technology systems under the oversight of the Company's Board of Directors.

Objective

To ensure that the implementation of information technology systems in business operations achieves the defined objectives, resources are used appropriately, and risks are managed properly, in alignment with good corporate governance standards (Corporate Governance).

Requirements

1. Establish a written policy for the governance and management of information technology, covering the following areas:
    1) Management of information technology risks, including risk identification, risk assessment, and implementation of controls to maintain risks at an acceptable level for the organization.
    2) Allocation and management of IT resources, ensuring sufficient resources to support business operations and establishing guidelines to address situations where resources are insufficient.
    3) Establishment of information security policies and measures to ensure compliance with the governance and management of information technology systems.

2. It is required to govern and manage information technology, covering the following topics:
    1) Communicate the IT governance and management policy to all personnel in an easily accessible manner, ensuring that staff understand and can correctly follow the policy.
    2) Establish procedures and work practices in accordance with the IT governance and management policy.
    3) Review or update the IT governance and management policy at least once a year, and immediately whenever any event or changes in laws and regulations may impact IT governance and management. Procedures and work practices must also be updated to align with any changes in the policy.

OSOTSPA	**Unit / Division :** Digital Technology	
	Document Type : Policy	
	Document Number : M-HM-ITD-001	**Revision :** 4
	Effective Date : May 1, 2025	**Page No. :** 6 of 29

Subject : Information Security Policy

Section 2 : IT Security

1. Guidelines for Information Security Measures

A written policy shall be established for the governance and management of information technology.

1. Information Asset Security
    1) Access Control
    2) Physical and Environmental Security
2. Information Management and Confidentiality
    1) IT Asset Classification to define appropriate security measures
    2) Data Backup
    3) Cryptographic Control
3. Personnel Oversight and Management
    1) End User Controls
        - Protection of Unattended User Equipment
        - Mobile Device and Teleworking
        - Installation of Software on Operational Systems
    2) IT Outsourcing Controls
4. Computer Network and Information Transfer Management
    1) Communications Security
    2) Information Transfer Control
5. Information Systems Threat Protection
    1) Protection From Malware
    2) Technical Vulnerability Management
6. System Acquisition, Development and Maintenance

2. Organization of Information Security

Objective

1. To control the implementation of information technology security duties across departments, ensuring compliance with the Information Security Policy.
2. To establish security measures for teleworking and the use of mobile devices to access internal systems.

OSOTSPA	**Unit / Division :** Digital Technology	
	Document Type : Policy	
	Document Number : M-HM-ITD-001	**Revision :** 4
	Effective Date : May 1, 2025	**Page No. :** 7 of 29

Subject : Information Security Policy

Requirements

1. Internal Organization
    1) Document IT security responsibilities in writing, specifying detailed duties to serve as a guideline for all relevant personnel across departments.
    2) Segregation of Duties — clearly separate responsibilities in IT security-related tasks to enable mutual review of work.
    3) Separate personnel and responsibilities between System Development and System Administration in the production environment to ensure proper oversight and control.
    4) Appoint delegates to perform tasks as backups, allowing work to continue in urgent or necessary situations.
    5) The Digital Technology Department shall designate contact persons for IT operations to coordinate and respond to incidents affecting information system security, and regularly review and update the contact list to keep it current.
2. Moveable Device: Computer Notebook, Mobile Device
    1) Register mobile devices (e.g., brand, model, operating system, serial number, and network identifiers such as IP/MAC addresses) before use. Review the registry at least annually and whenever devices are replaced, and revoke access for old devices.
    2) Protect sensitive data in case of lost mobile devices, e.g., require a lock screen password or enable remote data wipe.
    3) Define permitted application usage on mobile devices and restrict access to ensure secure network connections, such as limiting certain applications when connected to external networks.
    4) Encrypt critical information stored on mobile devices and transmitted over computer networks.
    5) Communicate the policy to users and obtain acknowledgment to raise awareness of risks and risk control measures.
    6) Control installation of authorized, licensed software to patch vulnerabilities and prevent malware, protecting information stored on mobile devices from unauthorized access or damage.
    7) Implement measures to mitigate impacts from security incidents, such as immediate revocation of access or disconnection upon detection of a threat.
3. Teleworking
    1) Establish appropriate physical security measures for external work locations, ensuring sufficient protection according to the scope of operations.
    2) Control user access rights to information based on their roles and responsibilities.
    3) Security of critical internal systems and computer networks in cases of remote connection or transmission of confidential or sensitive information (Remote Access), including the implementation of firewalls,

updating of anti-malware software, access control, and the use of data encryption or network encryption, as appropriate.

4) Implement a Data Leak Prevention (DLP) system to prevent unauthorized disclosure of information.

5) Assign user IDs and require password authentication to prevent unauthorized individuals (e.g., relatives, friends) from accessing information.

6) Regularly review and verify access rights of employees authorized to work via external networks.

7) Protect against malicious software such as malware and viruses.

4. Cloud Computing Usage

1) Establish a Cloud Computing Usage Policy, which shall at least cover the following aspects:

- Risk Assessment related to the use of cloud services.
- Define the types of work and service models to be used, such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
- Define the vendor selection and evaluation process (Due Diligence), with emphasis on the confidentiality of critical information (Confidentiality), data and system reliability (Integrity), and system availability (Availability).
- Conduct regular reviews of service provider qualifications, such as service capacity planning, to ensure that the provider maintains sufficient capabilities to support ongoing business needs.
- Communicate and disseminate the cloud usage policy to relevant employees and require acknowledgment to raise awareness of security concerns related to Cloud Computing usage.
- Clearly define the roles and responsibilities of the service provider, such as data backup.
- Establish procedures for issue reporting and resolution, including steps, escalation processes, contact persons, and communication channels.
- Define data security requirements for each type of data used in the cloud by classifying them according to the Information Safeguarding Guideline.
- Define appropriate security measures for each usage type to prevent threats and unauthorized access to information.
- Require the use of Multi-Factor Authentication (MFA) for accessing administrator pages of critical information systems.
- Establish audit and logging practices to monitor and track issues that may affect cloud services.

2) Define the agreement between the service provider and the service user, with the following characteristics:

- The service user retains ownership of the information.
- Define the types of services to be used within Cloud Computing.
- Establish network security standards, including data encryption for information transmitted over computer networks, protection against Distributed Denial of Service (DDoS) attacks, prevention of intrusion from

malicious software, protection against new and advanced threats (Advanced Persistent Threats — APT), network segmentation, application-level encryption, layered intrusion prevention (Defense-in-Depth), and hardening of information systems.

- Specify access control agreements, including methods for system access, assignment of user permissions, monitoring, issue resolution, error reporting, system performance, and overall system condition.
- Define the roles and responsibilities of the service provider, including data backup, issue resolution processes, Service Level Agreements (SLA), Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO), clearly specifying which types of data and the most recent datasets can be restored.
- Set conditions for liability in cases where the service provider fails to deliver services as agreed.
- Ensure that agreements include provisions related to data leak prevention, covering risks that may arise from the service provider.
- The service provider shall not access or disclose the service user's information unless authorized by the service user or as required by the laws of the cloud server hosting country or the provider's origin country, including national security regulations.
- The service provider should immediately update operations to comply with current international information security standards, such as ISO 27001.
- Include exit plan requirements when ending the use of services, such as specifying data retention periods and methods to destroy data to ensure it cannot be recovered.
- Specify conditions for using cloud services from subcontracted providers, ensuring such services are considered part of the main provider's responsibilities, and the main provider is accountable for any damages caused by subcontracted services.

3) Monitoring, evaluating, and reviewing the service provider's performance should additionally be conducted as follows:

- Monitor and review the performance of services, including security measures, to ensure compliance with contractual requirements or service agreements.
- Regularly assess the adequacy of the service provider's systems (Capacity Planning) to ensure they meet business needs.
- Review service conditions whenever changes occur to ensure the services remain aligned with usage requirements and information security policies.
- Continuously review the qualifications of the service provider, such as auditing operational processes and evaluating performance effectiveness.

3. Human Resource Security

Objective

To ensure that employees and external personnel with access to internal data or systems have the knowledge, understanding, and awareness to work in compliance with information system security.

Requirements

1. Provide IT security training for employees and external personnel.
2. Communicate to personnel and external parties to exercise caution, refrain from using information systems in ways that may harm business operations, and immediately report any significant information security incidents to the responsible authority.

   Examples of business operation damages include defamation, threats, impersonation, chain emails, and disclosure of confidential information.
3. Establish disciplinary measures for personnel who violate or fail to comply with the policy or related regulations concerning information technology system security.

4. IT Asset Management

Objective

1. To control information assets and the supporting infrastructure, including network connections, to ensure system security.
2. To protect and safeguard information assets appropriately, reducing the risk of unauthorized disclosure, alteration, or damage to data stored in any storage media.

Requirements

1. Responsibility for Assets
   1) The Digital Technology Department is responsible for managing and maintaining information assets, including hardware and software, throughout their entire lifecycle.
   2) All employees are responsible for the computers assigned to them, such as desktops and notebooks, and must ensure proper use and care of these assets throughout their life cycle.
   3) Responsibilities related to information assets must be reviewed and updated to align with the employee's role whenever there are changes in job responsibilities.
   4) The Digital Technology Department is responsible for managing information assets related to systems or equipment, including maintaining an asset register and conducting reviews at least once every three years, or whenever changes to the information assets occur.

2. IT Asset Classification

1) Establish security standards by classifying information and categorizing information assets according to their level of importance.

2) Data storage media management shall follow these practices:

- Implement standardized data destruction processes to prevent leakage and ensure irrecoverability when data is no longer required.
- Securely destroy storage media to prevent leakage of confidential or sensitive information.
- Define the lifecycle and reuse methods of storage media (e.g., servers, switches, media tapes, backup devices) in cases where data is stored for extended periods.
- Store data storage media in secure locations in accordance with the manufacturer's recommendations.
- Establish security measures for handling and protecting storage media during transportation outside the designated area.

5. Data Security

Objective

1. Ensure data accuracy, completeness, availability, and appropriate confidentiality.
2. Cover the entire data life cycle - from creation or acquisition, processing, storage, and usage to destruction- while clearly specifying data classification (labeling).

Requirements

1. Establishing individual responsibilities for information security for the entire workforce

1) All employees are responsible for protecting company data and must not disclose it to external parties or the public unless required by their job responsibilities. This ensures proper confidentiality and data management.

- Data Owner: The creator of the data is responsible for classifying, labeling, setting access rights, and ensuring its security.
- Data User: The individual authorized by the data owner to access the data must handle and manage it according to the confidentiality level set by the owner.

2. Data Classification

1) The data owner must classify data confidentiality, in both paper and electronic form, based on potential impact if disclosed.

Sensitivity Level	Definition	Sample data
For Public Use	Public information: Data approved for public release or distribution, with no access restrictions, containing no confidential, proprietary, or sensitive IT-related content.	Marketing materials, press releases, job announcements, and reports published for public access.
Confidential (Internal and OSP Partner Use)	Internal company information accessible to authorized external parties, containing confidential content that should not be disclosed or published publicly. For sensitive personal data, apply masking or encryption before sharing.	Agreements with suppliers, quotations, purchase orders, project documents with contractors, and HR information shared externally as required by regulations or for employee benefits.
Confidential (Internal Use Only)	Internal company information that is confidential and must not be disclosed outside the organization. If external access is necessary, confidential data should be masked before downgrading its classification for sharing.	Internal policies and procedures, company internal announcements, employee performance evaluation documents, HR information not required to be shared externally, sales targets, and internal audit reports.
Highly Confidential (Restricted Distribution)	Highly confidential information accessible only to authorized personnel on a need-to-know basis. Unauthorized disclosure may cause financial, legal, or regulatory harm, or negatively impact the company's reputation.	Executive-level business plans, merger and acquisition plans, and trade secrets, such as manufacturing formulas.

3. Data Labeling and Handling

1) For electronic data, the following actions must be performed at a minimum:

Data Management	Confidentiality Levels			
	For Public Use	**Confidential (Internal and OSP Partner Use)**	**Confidential (Internal Use Only)**	**Highly Confidential (Restricted Distribution)**
Labeling	-	Clearly display on screens, storage media, and electronic messages.	Clearly indicate on display screens, storage media, and electronic messages.	Clearly display on screens, storage media, and electronic messages.
Authentication	-	Authentication is required.	Authentication is required.	Multi-Factor Authentication is implemented.
Access Control	-	Accessible only to employees and authorized external personnel.	Accessible only to employees.	Accessible only to employees and authorized external personnel
Data in Transit	-	Data is encrypted.	Data is encrypted.	Data is encrypted.
Data at Rest	-	Data is encrypted.	Data is encrypted.	Data is encrypted.
Data destruction on storage media.	-	Destroy data to ensure it cannot be recovered.	Destroy data to ensure it cannot be recovered.	Destroy data to ensure it cannot be recovered.

2) For data in document form, follow the company's document management policy.

6. Access Control and Network Security

Objective

1. To establish standards for data access control and facilitate system data processing.
2. To manage information system access rights appropriately according to job responsibilities.
3. To prevent unauthorized individuals from accessing the information system.
4. To safeguard information systems and applications from unauthorized access and ensure IT security.

Requirements

1. Business Requirement of Access Control

    1) Assign access rights to information and IT systems according to user responsibilities, regularly review these rights, and promptly revoke access for individuals without necessity.

    2) Implement segregation of duties for relevant personnel, such as access requesters, access authorizers, and access administrators. If segregation is not feasible, alternative controls like monitoring operations and reviewing audit evidence by supervisors or unrelated personnel must be applied.

    3) Define network access controls, including permitted network services, authorized users, access control processes, secure access methods, authentication techniques, and activity monitoring for authorized users.

    4) Maintain a system that clearly identifies users on the computer network, including mapping dynamic IP addresses to users to track who accessed the network at specific times.

2. User Access Management

    User accounts are managed to restrict access to information, allowing only authorized individuals to access it, as follows:

    1) User accounts are registered according to approved roles and responsibilities.
    2) High-level access rights are limited and carefully controlled.
    3) Passwords are managed following international standards.
    4) Access rights are regularly monitored and reviewed at least once a year.

3. User Responsibilities

   1) Access to the system is assigned based on User ID, and each user is responsible for all actions performed under their User ID.
   2) Users must follow usage procedures and maintain the security of their passwords.
   3) Users are accountable for their User ID, password, and any personal information used to modify their account.

4. System and Application Access Control

   Access to information systems and applications is protected against unauthorized use as follows:

   1) Control access to and usage of information and functions within applications for both users and system administrators according to assigned permissions.
   2) Implement secure password management, restrict use of utility programs, and limit access to program control commands.
   3) Prevent access through guessing or brute-force attempts, and regularly maintain and review login attempt logs.
   4) Ensure practices comply with established access control requirements.
      - Each user is responsible for their own User ID and password.
      - Every user must have a unique User ID and password to authenticate their identity.
      - Users must change the initial password provided by IT immediately; the new password must be at least 8 characters long, containing lowercase and uppercase letters, numbers, and special characters, or as required by the system.
      - Users can set or change passwords themselves, following a verification process.
      - Passwords must be changed upon first use and at least every 90 days, or as specified by the system.
      - New passwords should not repeat any of the last six used passwords, or as specified by the system.
      - Passwords must not be displayed on-screen while being entered.
      - Passwords must be encrypted to prevent unauthorized access or modification, and stored separately from application data.
      - After more than six failed login attempts, or as defined by the system, the account must be locked; unlocking is done by IT or automatically with supervisor approval.
      - Passwords must be securely delivered to users, e.g., sealed envelopes.

7. Cryptographic Control

Objective

To ensure that system usage includes proper data encryption (Cryptography) and key management (Key Management) in accordance with international standards, maintaining appropriateness and efficiency, while preventing unauthorized access, alteration, or modification of confidential or business-critical information.

Requirements

1. Policy on the Use of Cryptographic Controls
    1) The Digital Technology Department must ensure data encryption matches the required confidentiality level.
    2) The cryptographic algorithms used must comply with international standards, such as AES-128 for symmetric key encryption and RSA-2048 for asymmetric key encryption.
    3) The encryption methods must be regularly reviewed at least once a year to ensure that they remain sufficiently secure for protecting information.
2. Key Management
    1) Key Generation and Installation should be carried out at least as follows:
        - Control the environment and process of key generation to ensure strict security, e.g., use a trusted Certification Authority and destroy any residual data after key creation to prevent unauthorized access or recovery.
        - Restrict access to encryption keys only to authorized personnel.
        - Ensure encryption key length is sufficient to prevent decryption attempts such as brute force attacks.
        - Perform key exchange through secure processes and channels.

    2) Key Storage and Backup should be carried out at least as follows:
        - Ensure secure storage of encryption keys through both physical protection and appropriate access control.
        - Maintain backup copies of encryption keys with the same level of security as the primary keys.

    3) Revocation or Destruction of Encryption Keys should be carried out at least as follows:
        - Define criteria and guidelines for key replacement or revocation, such as when keys expire or are deemed insecure.
        - Establish a secure destruction process to ensure revoked keys cannot be reused.

    4) Logging of Key Management Activities should be maintained, including key generation, backup, access or usage, and revocation.

8. Physical Security of Data Center Management

Objective

1. To prevent unauthorized individuals from accessing secure areas (e.g., Data Center, Backup Site, Floor Switch, Router), which could cause damage to IT equipment or compromise confidential or critical information.

2. To protect information assets and equipment from loss or damage due to unauthorized access or misuse, and to ensure their continuous operation.

Requirements

1. Restricted Areas

   1) Designate data centers, network equipment areas, and information asset storage as Restricted Areas.

   2) Design restricted areas with protection against natural disasters, human threats, and unauthorized disclosure of details to the public.

   3) Limit access rights to authorized personnel only, implement strict access control, and review rights regularly.

   4) Provide security measures in data centers, such as CCTV, fire alarms, fire extinguishers or automatic suppression systems, UPS or backup generators, and proper temperature/humidity control, with regular maintenance.

   5) Closely monitor and control third parties (e.g. suppliers) or unauthorized individuals working in restricted areas.

   6) Separate delivery/receiving areas from the data center.

   7) Store critical IT equipment, such as servers and network devices, securely within restricted areas.

2. Information assets in the form of hardware equipment

   1) Implement protection for hardware information assets against disruptions caused by failures in infrastructure systems, such as power, telecommunications, ventilation, and air-conditioning systems.

   2) Ensure secure protection and regular maintenance of communication cables, power lines, and related equipment (e.g., floor switches, cable conduits) to prevent damage.

   3) Label all equipment within communication equipment racks (Rack Servers).

   4) Label all equipment within communication Prevent unauthorized removal of hardware assets from premises; if authorized, maintain an asset register and appropriate security measures according to the risk level of offsite usage. racks (Rack Servers).

   5) Control computer screens to prevent sensitive information from being visible when not in use, through measures like automatic screen lock or session timeouts.

6) Ensure security of hardware assets when not in use, including control of documents or storage media such as thumb drives and external hard disks, preventing them from being left on desks or unsecured areas.

7) Maintain hardware assets properly to preserve accuracy, completeness, and operational readiness.

8) When decommissioning or disposing of network hardware assets (e.g., switches, firewalls, routers), ensure all configuration data is erased, moved, or reset to factory defaults according to standards to prevent recovery.

9. Operations Security

Objective

1. Ensure that information system operations are conducted correctly and securely.
2. Protect information systems from malware, technical vulnerabilities, and data loss.
3. Record and store sufficient evidence of system usage for auditing, monitoring unauthorized access, and investigating abnormal or non-compliant activities.
4. Ensure system operations are accurate, complete, and reliable (Integrity of Operational System).

Requirements

1. Operational Procedures and Responsibilities

1) Establish operation manuals for information systems to guide staff in correctly performing tasks such as system start-up/shutdown, processing, performance monitoring, and scheduling. Ensure these manuals are regularly reviewed, kept up to date, and easily accessible.

2) Strictly control operations, especially when system structures, procedures, or workflows change, which may affect information security. This includes:

- Documented procedures for changes, including backup plans and post-change testing.
- Assessment of potential impacts and approval from authorized personnel.
- Verification that changes comply with information security policies.
- Communication to relevant personnel for correct implementation.
- Fall-back procedures to restore systems in case of errors during changes.

3) Monitor the performance of information systems and critical IT equipment to ensure continuous, efficient operation. Use this data to assess system capacity and capability, supporting effective planning for future operations.

4) Segregate computers used for system development (Development Environment) from those used in live operations (Production Environment), and restrict access in each environment to authorized personnel only.

2. Protection From Malware

1) Prohibit the use of unauthorized software.

2) Install firewalls to prevent and monitor unauthorized software usage and access to unsafe websites that may contain malicious programs.

3) Deploy anti-malware software and keep it regularly updated, assigning responsible personnel to report and remediate detected threats.

4) Regularly audit critical system software, and immediately investigate any unauthorized installations or changes.

5) Monitor and filter threat intelligence to stay informed of actual risks and raise awareness among relevant personnel.

3. Backup Data

1) Establish detailed backup procedures to prevent data loss and guide personnel, specifying:

- Data to be backed up
- Backup frequency
- Number of backup copies
- Media type, storage location, and handling methods
- Step-by-step backup process
- Data recovery procedures in case of loss

2) Store backup media and procedure copies offsite to ensure safety if the primary site is damaged, with proper access control and damage-prevention measures.

3) Define data recovery objectives, specifying the types of data and the most recent data set that can be restored (Recovery Point Objective: RPO).

4) For long-term storage, plan for data retrieval by considering the media type, and ensuring required devices and software to access the stored data are available.

4. Logging and Monitoring

1) Implement a system to log and store evidence of information system usage, including creation, modification, and changes, ensuring completeness for auditing and preventing unauthorized access or data damage.

2) Protect logs, including general user, system administrator, and system operator logs, from alteration, damage, or unauthorized access, and review them at least annually or whenever changes occur.

3) Configure clock synchronization for critical devices and information systems to align with international time standards.

4) Maintain logs that record significant system events as evidence.

No.	Types of Evidence Storage	Evidence Storage Details	Retention Period
1	Physical Access Log	Person who accessed / date and time of access / access attempts (if any)	Not less than 90 days
2	Access logs for operating systems, databases, and computer networks (Authentication Log)	User account / date and time of access / access attempts	Not less than 90 days
3	Access and activity logs for information systems (Application Log)	User account / device identifier (IP Address) / date and time of usage. It must be possible to identify the user and the local IP address during the session (for company-issued devices only), subject to the system or application-specific conditions.	
4	Internet usage logs via internal computer network (Internet Access Log)	User account / device identifier (IP Address) / organization IP Address / date and time of usage / destination website address (Full URL). It must be possible to identify the user and the IP Address during the session.	Not less than 90 days
5	Audit Log	User account / date and time of access / records of data viewing and modifications.	Not less than 90 days
6	Administrative log (Event Log of Operating System and Network Firewall)	Date and time of the event / Event occurring on the OS (Event Services), such as service status / Event occurring on the Network Firewall, such as updates or modifications of Firewall Rules	Not less than 90 days
7	Network Firewall traffic log (Network Firewall Log)	Date and time / Source and destination IP address / Firewall action / Port used	Not less than 90 days

No.	Types of Evidence Storage	Evidence Storage Details	Retention Period
8	Database Management Log	User account / Login date and time	Not less than 90 days
9	Electronic Messaging	User account / Login date and time / Contact information throughout the session	Not less than 90 days

5. Control of Software Installation on Operational Systems

   Control software installation and restrict installation rights for users to ensure operational systems maintain integrity, accuracy, and reliability.

6. Technical Vulnerability Management

   1) Conduct penetration testing on critical operational systems by internal or external experts independent of the IT department, in accordance with risk and business impact analysis.

   - High-priority critical systems connected to public networks (Internet-facing) must be tested at least once a year and whenever significant changes occur.
   - Other important systems should have a risk assessment for potential intrusions via internal network communication to define the appropriate scope of penetration testing.

   2) Conduct vulnerability assessments on all critical systems at least once a year and whenever significant changes occur.

   3) Remediate identified vulnerabilities immediately, assessing program risks before installation, testing, and evaluating potential impacts of the installation.

   4) Implement a technical vulnerability management process aligned with the Incident Management process to prepare for and respond to system breaches via vulnerabilities.

   5) Record and store evidence to audit all actions related to technical vulnerability management.

7. Information System Audit

   1) Plan information system audits in accordance with assessed risks.

   2) Define the technical audit scope to cover critical risk points, ensuring the audit does not disrupt normal operations.

   3) Conduct audits outside working hours if the audit may impact system availability.

10. Communications Technology Security

Objective

1. To prevent actions that pose risks to information on the computer network and to protect the infrastructure supporting the network operations.
2. To ensure the security of information transmission within the internal network and between the internal and external networks.

OSOTSPA	**Unit / Division :** Digital Technology	
	Document Type : Policy	
	Document Number : M-HM-ITD-001	**Revision :** 4
	Effective Date : May 1, 2025	**Page No. :** 22 of 29

Subject : Information Security Policy

Requirements

1. Network Security Management

   1) There is secure management and control of the computer network system, ensuring prevention of actions that could pose risks to information transmitted through the network.
   2) Define segmentation of the computer network, clearly specifying the scope of each subnet and controlling access appropriately to align with the security requirements of each segmented area.
   3) Separate responsibilities among the Network Administrator, Server Administrator, and Computer Administrator, assigning access rights according to roles and responsibilities, with clear procedures for managing network systems and devices.
   4) Control connections to public networks and wireless networks, requiring all users to authenticate via User Login through Active Directory (AD) Authentication to prevent data leakage or unauthorized modification of information transmitted over these networks.
   5) Implement firewalls to protect connected systems and applications, ensuring separation between different network segments.
   6) Limit connections between networks, such as restricting port usage between servers and clients, enabling only necessary service ports, and clearly authenticating connected devices (e.g., IP address and device type).
   7) Provide a redundant computer network system (Network Load Balance) to maintain availability and minimize business disruption.
   8) Regulate external network access: users connecting from outside the organization or via mobile devices (e.g., notebooks or smartphones) must authenticate through designated channels before accessing the network.
   9) Maintain network logs to monitor and track abnormal activities, ensuring the ability to audit operations that may impact network security.
   10) Establish agreements with external service providers for network usage to ensure the security of the computer network.

2. Information Transfer Control

   1) Establish guidelines for the secure transfer of information both within the organization's internal network and between the internal network and external networks:
      - Provide procedures for transferring information through various types of electronic communication channels.
      - Implement measures to prevent information from being transmitted outside designated routes, intercepted, altered, damaged, or affected by malicious programs (malware) during transmission.
      - Implement processes to protect confidential or critical information sent as attachments or automatically forwarded via email to external recipients (Data Leak Prevention).
      - Apply encryption techniques for transferring confidential or critical information over communication channels that require security, such as when using cloud computing systems.

OSOTSPA	**Unit / Division :** Digital Technology	
	Document Type : Policy	
	Document Number : M-HM-ITD-001	**Revision :** 4
	Effective Date : May 1, 2025	**Page No. :** 23 of 29

Subject : Information Security Policy

2) Information Security Measures for Data Transfer via Computer Networks

- Implement protections to prevent unauthorized modification, access, or tampering of information.
- Manage and control systems to ensure data transfer operations are accurate and consistently available.
- Ensure the security of information when sending data or messages via email or other electronic communication channels.
- Require approval for using information transfer systems provided by external parties.

3) Use of Information Transfer Systems via Computer Networks (Electronic Messaging)

- Implement measures to prevent unauthorized modification, damage, or access to information.
- Require user authentication each time access occurs through public networks.
- Control the use of external services for transferring information via computer networks, including:
  - Instant Messaging applications and social networking platforms (e.g., LINE, Facebook, Instagram, WhatsApp).
  - Cloud-based file sharing applications (e.g., OneDrive, Google Docs, Dropbox).

  Use of these applications must be approved solely by the agency's top management, and the Digital Technology Department is responsible for strict control (Control List).
- Users must comply strictly with applicable laws and regulations.

4) Establish confidentiality or non-disclosure agreements (Confidentiality or Non-Disclosure Agreements) for internal users and contractors. They must sign agreements to protect information critical to information technology security.

- Identify ownership of critical business information, intellectual property, and methods to prevent data leakage.
- Ensure prevention of unauthorized disclosure by requiring signatures from responsible parties.
- Define procedures for requesting access to information or specify access rights according to the signed agreement.
- Specify access rights for monitoring, tracking, and auditing the use of critical information.
- Establish alerts and reporting to relevant parties if unauthorized disclosure or leakage occurs.
- Define enforcement measures in case of violation or termination of the agreement, including requirements for returning or securely destroying critical information at the end of the agreement.

11. System Acquisition, Development and Maintenance

Objective

1. To ensure that the processes and procedures for information systems operations follow a clear, standardized work methodology and maintain security for business operations, covering the entire lifecycle from procurement, system development, usage, to maintenance.
2. To ensure that the development or modification of information systems is accurate, complete, efficient, and meets user requirements (Change Management).
3. To reduce errors and prevent data loss, as well as incorrect modifications that may occur in the information systems.
4. To maintain the security and integrity of information systems throughout the system development life cycle (System Development Life Cycle: SDLC).

Requirements

1. Security Requirements of Information Systems
   1) There are requirements for procuring, developing, and maintaining information systems to ensure security, whether it is a new system or an enhancement of an existing system.
   2) There is protection of information security in cases where access is made to application services.
2. Security in Development and Support Process
   1) Control of Development or Changes to Information Systems
      - Requests for system development or modification must be submitted in writing by the relevant department or user and approved by authorized personnel to control potential side effects of the changes, such as by the Business Process Owner (BPO).
      - Conduct a risk assessment or evaluate potential impacts arising from the development or modification of the system.
      - Control personnel, procedures, and IT resources throughout the system development process.
      - Monitor and control the system development performed by service providers to ensure compliance with service agreements, including maintaining the confidentiality of processed data, controlling data input/output in development systems, and strictly managing access to the development environment. Track any changes to the development environment.
      - In cases where external organizations or individuals are contracted to develop the system, supervision, monitoring, and tracking of the outsourced development process must be implemented to ensure compliance with IT security policies.
   2) Establish written procedures for developing, modifying, or changing operational systems, including requirements for requests, development, modification, testing, and the process of migrating the system into production use.
      - Separate computers or applications used for system development (Development Environment) from those used in production (Production Environment), assigning access rights and controlling access only to authorized personnel or those involved in each environment.

3) Establish procedures for emergency changes to computer systems (Emergency Change), requiring approval from authorized personnel each time.

4) Require testing of developed or modified information systems by users or independent testers, separate from the developers, to ensure that the systems operate efficiently, process data accurately and completely, and meet user requirements.

5) Ensure the Business Continuity Management plan is updated to reflect any development, modification, or changes to the information system.

6) Maintain versions of developed programs and accompanying system development documentation:
   - Store detailed information on current programs, including records of development, modification, and changes.
   - Update system documentation after development or modification to keep it current, and store it securely while remaining accessible.
   - Retain previous program versions prior to modifications for possible rollback (Fall-Back) if the system malfunctions or becomes unusable.

7) Communicate all system changes thoroughly to relevant users to ensure correct usage.

8) Record and store all evidence related to system changes for audit and verification purposes.

12. Provision of Information Technology Services by Outsourced Providers (IT Outsourcing)

Objective

1. To establish requirements and operational guidelines for receiving or utilizing outsourced IT services, ensuring alignment with objectives, efficiency, and the security of the information system (Information Security).
2. To protect information assets from inappropriate access by the service provider.
3. To control the service provider to ensure the delivery of work is accurate, complete, and in accordance with the agreed terms.

Requirements

1. Information Security in IT Outsourcing

   1) Establish the classification of service providers (IT Outsourcing Classification) and assess the risks associated with each provider (IT Outsourcing Risk Assessment) to provide guidelines for managing each type of provider and to minimize potential future risks.

   2) Define the selection and evaluation process for service providers (Due Diligence), with emphasis on information confidentiality (Confidentiality), accuracy and reliability of information and information systems (Integrity), and availability of the information systems being serviced (Availability).

   3) Set written guidelines for overseeing service providers to reduce the risk of inappropriate access to information assets, and regularly review the qualifications of providers to ensure they remain capable of delivering services sufficiently to support continuous business operations.

4) Establish a Non-Disclosure Agreement (NDA) or a data confidentiality agreement, clearly specifying the scope of work and the conditions of service delivery (Service Level Agreement: SLA). The agreement must be jointly signed by the authorized signatory and the service provider.

5) Define the responsibilities of the service provider and specify the types of information they are authorized to access. Implement appropriate procedures, controls, and monitoring of data access based on the principle of necessity.

6) Ensure the security, integrity, and accuracy of information during its transfer and processing by the service provider.

7) Ensure the security, integrity, and accuracy of information during its transfer and processing by the

8) Regularly track, review, and audit the service provider's operations and service performance.

9) If the service provider modifies processes, procedures, or operational practices related to information security, assess the risks associated with such changes and adjust risk management processes accordingly.

10) When changing service providers, evaluate their performance as necessary and consider any potential risks that could impact business operations during the transition.

11) The agreement regarding the security of information technology systems includes the following:
- Details of the information necessary for access by the service provider, including methods of accessing the data.
- Classification of information according to data levels, in accordance with the Information Safeguarding Guideline.
- Measures to ensure that confidential or critical information, intellectual property, and copyrights are securely protected in compliance with the law.
- Responsibilities of the service provider under various controls, such as defining access conditions, monitoring compliance with agreements, and requiring the provider to report on performance and resolve issues within specified timeframes.
- Guidelines for the proper and appropriate use of information.
- Contingency plans for incidents that could affect the security of information systems.
- Contact names and channels for relevant individuals or departments, particularly those responsible for IT system security.
- Additional requirements for IT system security in cases where the service provider delegates tasks to another party (Sub-Contracting to Another Supplier).

2. Supplier Services Delivery Management

1) Service Service providers shall be regularly monitored, reviewed, and audited, with risk assessments and management in place for any changes to their processes or operations.

2) For system development services, providers may only access the Development Environment. Any necessary access to the Production Environment must be strictly controlled and closely supervised to

ensure compliance with defined scopes.

3) For onsite services, authorized staff must closely monitor the provider's work.

4) For remote access services, access duration must be clearly defined and terminated immediately after service completion.

5) Providers must prepare operation manuals and relevant documents prior to work handover.

6) Providers must report work performed, encountered issues, and corrective actions.

7) Work acceptance procedures must verify accuracy and compliance with agreed conditions.

13. Information Security Incident Management

Objective

1. To ensure that incidents and vulnerabilities related to information system security are properly investigated, corrected, and resolved promptly and effectively within an appropriate timeframe.
2. To enable relevant personnel to learn from issues that occurred, implement corrective actions, and prevent similar security incidents in the future.

Requirements

1. Establish procedures and processes for managing incidents that may affect the security of information systems.
   1) Define a documented contingency plan in case of incidents.
   2) Assess incidents or weaknesses in information security measures and determine their severity and potential impact on system security.
   3) Assign a designated point of contact (POC) to receive incident reports and escalate them to management or relevant parties.
   4) Implement effective response actions to contain and resolve incidents, ensuring a rapid return to normal operations.
   5) Collect and securely store evidence immediately when incidents affect critical systems (e.g., customer data or assets), with clear responsibilities assigned for analysis, investigation, and reporting.
   6) Record and store incident management documentation as necessary and appropriate.
   7) Detect, monitor, analyze, and report incidents, including post-incident analysis to identify root causes and apply lessons learned for future preparedness.

2. Define personnel responsible for managing incidents that may affect information system security.
3. Ensure incidents are reported to those responsible for managing information system security.
4. Regularly review and test incident management procedures, including conducting a Cyber Security Drill at least once a year.

   Explanation:
   A Cyber Security Drill refers to threats that may impact, damage, or pose risks to business operations arising from the use or application of computer networks, the internet, telecommunications networks, etc.
5. Evaluate test results and review processes, with findings reported to management. Such evaluations must be carried out by personnel independent from those directly responsible for incident management.
6. Maintain incident management records and related evidence for at least two (2) years from the date of creation, stored in a manner that allows immediate retrieval and inspection.

14. Information Security Aspects of Business Continuity Management

Objective

1. Ensuring integrity to integrate information security into Business Continuity Management (BCM), ensuring information systems are always available and ready for use.
2. To support continuous business operations and minimize impacts during emergencies or disruptive incidents affecting information systems.
3. To protect critical business processes from failure, interruption, or emergency situations that could affect information system operations, ensuring continuity.
4. To enable rapid recovery of information systems to normal operations without adverse effects on business continuity.

Requirements

1. Establish Measures for Handling Information System Emergencies
   1) Define information security requirements and potential damage scenarios, such as natural disasters or political crises.
   2) Identify critical systems, applications, and processes essential to business operations.
   3) Back up data to ensure accuracy, integrity, and availability, with regular testing of backup data. The backup format and frequency should be determined based on business needs.
   4) Develop a formal written emergency response plan covering operational plans, processes, procedures, coordination with relevant stakeholders, and adaptation to changing work environments.

5) Develop an emergency response plan aligned with the Business Continuity Management (BCM) plan, including regular testing and reporting of test results to relevant stakeholders. The plan shall be tested at least once a year.

2. Establish procedures, processes, and controls related to information system security in alignment with the Business Continuity Management (BCM) plan.

1) Define the participants for testing the Disaster Recovery Plan (DRP), including both internal and external parties, depending on the scenario being simulated for each disaster event, and invite them to participate in the emergency response testing.

2) Conduct regular reviews, updates, and improvements of the emergency response plan, operational processes, and procedures for continuously improving information security systems at least once a year to ensure the plan remains current, provides clear guidance, and meets the defined standards of information system security continuity. This is to ensure that the established measures remain valid and effective in the event of a disruptive incident.

3. Define recovery time objectives (RTO) and prioritize the restoration of information systems based on potential impacts.

1) Ensure regular checks on the readiness of information processing equipment.
2) Establish recovery timeframes for restoring information systems to normal operations.
3) Prioritize the recovery of all critical information systems in accordance with their potential impacts.
4) Maintain backup systems to ensure constant availability and readiness.

4. Maintain backup information systems in readiness to support recovery within the defined timeframe for resuming normal operations.

1) Establish backup data centers and backup information systems, with detailed specifications of backup sites or maps, to ensure business continuity and minimize impacts during emergencies.
2) Specify the required equipment for each system in emergency situations, including computer models, hardware specifications, configurations, and network devices.
3) Define the roles and responsibilities of relevant personnel in supporting the implementation of the Disaster Recovery Plan (DRP), including conditions for its activation.
4) Establish recovery timeframes and prioritize the restoration of all critical information systems in accordance with potential impacts.