Announcement

ITG 001/2567

Information Technology Management and Security Policy

The company has established the Information Technology Management and Security Policy and related guidelines to serve as standards and practices for the company's information technology systems to be appropriate, efficient, secure, and continuously improving information security systems. This includes preventing problems that may arise from incorrect use of information systems and threats from various dangers, both internal and external, whether intentional or unintentional, thereby reducing various damages and maintaining the ability to operate efficiently. This is also to comply with the Personal Data Protection Act B.E. 2562 (2019), the Computer-Related Crime Act B.E. 2560 (2017), and other relevant laws. The aforementioned operations will be measures to elevate the company's information technology security to international standards, by referencing operations according to the international frameworks ISO/IEC 27001, ISO/IEC 27701, and adopting guidelines from the Charoen Pokphand Group's Information Security Policy and Guidelines.

1. Scope

This announcement shall apply to CP All Public Company Limited and its subsidiaries (excluding CP Axtra Public Company Limited and companies within the CP Axtra Public Company Limited group).

2. Definition	**meaning**
"Company"	CP All Public Company Limited and its subsidiaries
"Subsidiaries"	CP All Public Company Limited and its subsidiaries (excluding CP Axtra Public Company Limited and companies within the CP Axtra Public Company Limited group)

“IT Task Group”	The Working Committee shall be responsible for establishing the information technology policy framework and presenting it to the Group Information Technology Committee (Ex-0+)
“Employee”	Employee who is hired to operate as a probationary employee, permanent employee, special contract employees and executives at all levels within Company employment
“User”	Directors, executives, department managers, employees, temporary staff, and any authorized individuals who are granted access to use, manage, or maintain the company's information systems in accordance with their rights and responsibilities
“Information Owner”	Organizational units accountable for company data, including their respective supervisors. These units are responsible for the data or would be directly impacted if that data were lost
“Data Subject”	Individuals who are the owners of personal data, including but not limited to customers, employees, and partners who provide personal data to the company
“Business Owner”	Organizational unit assigned oversight and responsibility for a particular business activity
“Infrastructure”	Individuals responsible for maintaining system infrastructure to ensure continuous operation in accordance with agreements. This includes the care of machines, operating systems, platforms, and networks, both On-Premise/Cloud

“IT Service Desk”	IT Help Desk (or IT Service Desk) which handles IT issues, e.g., Hotline 1500
“IT Systems Management”	Assigned IT System Custodians, such as Go Soft (Thailand) Co., Ltd. and the Information System & Service (ISS) Department
“Third Party/External Service Providers / External Party	Third-party users or external service providers with occasional or contractual access to the company's information systems, including: Business Partner, Outsource, Supplier, Service Provider, Consultant Business
“Internal Systems”	Company operations, including business activities and IT systems
“Information System”	Information systems that leverage technology to generate information usable for planning, management, service support, development, and communication control. These systems comprise computer technology and telecommunications technology, including computer systems, networks, software, data, and information
“Data”	Information conveying facts, regardless of how it's expressed or the medium used. This includes, but isn't limited to, information on CDs, DVDs, hard drives, thumb drives, documents, reports, books, maps, diagrams, drawings, photographs, computer records, or any other method that makes the recorded information accessible
“Information System Workspaces”	Areas where the company permits the use of information systems, categorized as follows:

	1. Secured Areas: These are spaces with controlled access and systems in place to protect against various threats 2. Working Area: Includes meeting rooms and general employee workspaces 3. General Access Areas: These are spaces designated for receiving external visitors to the company."
“Network System”	Systems capable of communication or data transfer between computer systems, including but not limited to: LAN (Local Area Network), WLAN (Wireless LAN), and Intranet systems

3. Roles and Responsibilities

3.1 Duties of the Managing Director and Chief Executive Officer (MD&CEO)

3.1.1. Define the vision, approve the company's operational plans, and drive the execution of those plans. This includes providing recommendations for operations and various investments to support the company's activities in line with the Information Security Management Policy.

3.1.2. Ensure appropriate information security governance to comply with the company's laws, regulations, policies, strategic plans, and operational plans.

3.1.3. Consider and approve the Information Security Policy.

3.2 Duties of the Chief Information Officer (CIO)

3.2.1. Define the goals and Information Technology Management and Security Policy in alignment with the Company's strategic plan.

3.2.2. Manage and develop the Information Technology Management and Security Policy, Standards, Procedures, and Guidelines to ensure the Confidentiality of information, the Integrity of information, and the Availability of systems.

3.2.3. Assess the need for IT resources, their cost-effectiveness, and procure and develop information systems in line with the Company's strategy.

3.2.4. Oversee the Company's information technology resources to efficiently support internal operations.

3.3 Duties of the Cyber Security Officer (CSO)

3.3.1. Participate in defining the goals and Information Technology Management and Security Policy for the Company, ensuring alignment with the Company's strategic plan.

3.3.2. Manage and monitor system attacks and various threats that may occur to systems, and plan business continuity for system recovery in emergencies.

3.3.3. Manage and analyze risks that may cause problems affecting the Company's business operations.

3.3.4. Present operational plans, policies, budgets, and staffing to senior executives such as the MD&CEO and CIO.

3.3.5. Be prepared for situations and continuously learn new techniques in information security.

3.4 Duties of the Data Protection Officer (DPO)

3.4.1. Participate in defining the goals and Information Technology Management and Security Policy for the Company, ensuring alignment with the Company's strategic plan.

3.4.2. Oversee units in managing and analyzing personal data risks that may affect data subjects and the Company's business operations.

3.4.3. Oversee units in preparing for the management of personal data breaches or leakages.

3.5 Duties of Commanders

3.5.1. Clarify and encourage users to comply with the Information Technology Management and Security Policy, and issue warnings or disciplinary actions in cases of inappropriate conduct.

3.6 Duties of Users

3.6.1. Must learn, understand, and strictly comply with the Company's Information Technology Management and Security Policy.

3.6.2. Fully cooperate with the Company in protecting its computer systems and information, monitoring and safeguarding the Company's data and information to ensure their security.

3.6.3. Report immediately to the Company when equipment or critical information is lost, or when intrusion, theft, destruction, or embezzlement of information is detected, including any damage caused to the Company.

3.7 Duties of Data and Information Owners

3.7.1. Arrange for the preparation of documents, measures, and procedures to control data access in accordance with the Company's Information Technology Management and Security Policy.

3.7.2. Ensure that employees comply with the Company's Information Technology Management and Security Policy.

3.7.3. Control and approve access to data, information, and computer systems under their duties and responsibilities.

3.7.4. Report security incidents related to data and information.

3.7.5. Notify the IT unit responsible for user account and system access rights management to delete/change rights when there are changes in employees / authorities / transfers.

3.8 Duties of the Internal Audit Department

3.8.1. Must establish audits of information security management, operations, and compliance as necessary.

4. The Company has established key Information Technology Management and Security Policies, which comprise:

4.1 Organization of information security and privacy controls

4.1.1. Threat intelligence management.

4.1.2. Information security in project management.

4.1.3. Inventory of information and other associated assets.

4.1.4. Information classification and labelling.

4.1.5. Information transfer.

4.1.6. Access and authentication management.

4.1.7. Supplier management.

4.1.8. Information security for use of cloud services.

4.1.9. Information security incident management.

4.1.10. Business continuity management.

4.1.11. Legal, statutory, regulatory and contractual requirements.

4.1.12. Protection of records.

4.1.13. Privacy and protection of PII.

4.1.14. Independent review of information security.

4.1.15. Documented operating procedures.

4.2 Human resource security

4.2.1. Human resource security.

4.2.2. Remote working.

4.2.3. Information security event reporting.

4.3 Physical controls

4.3.1. Physical and environmental security.

4.3.2. Clear desk and clear screen.

4.3.3. Storage media.

4.3.4. Secure disposal or re-use of equipment.

4.4 Technological controls

4.4.1. User endpoint devices.

4.4.2. Secure authentication and access control.

4.4.3. Capacity management.

4.4.4. Protection against malware.

4.4.5. Management of technical vulnerabilities.

4.4.6. Configuration management.

4.4.7. Information deletion.

4.4.8. Data masking.

4.4.9. Data leakage prevention.

4.4.10. Information backup.

4.4.11. Redundancy of information processing facilities.

4.4.12. Logging.

4.4.13. Monitoring activities.

4.4.14. Clock synchronization.

4.4.15. Installation of software on operational systems.

4.4.16. Networks security management.

4.4.17. Use of cryptography.

4.4.18. Secure development.

4.4.19. Testing Information.

4.4.20. Protection of information systems during audit testing

Remark: The Information Security Management Policy is detailed in Appendix 1.

5. Policy Review

Senior executives in information technology or personnel assigned for reviews must carried out policy reviews regularly at least once yearly and must be submitted to the Executive Committee Chairman for approval upon changes.

6. Violations and Penalties

All employees must comply with this policy. In the event of an investigation, full cooperation with internal and external units is required. Any direct or indirect violation or non-compliance with this policy will result in disciplinary action according to the Company's work regulations. If the act constitutes a legal offense and/or causes damage, the individual will be subject to legal penalties corresponding to the offense committed. If such an event causes damage to the Company and/or any other person, the Company may consider pursuing further legal action and claim full compensation for the damages incurred.

This will be effective from October 15, 2024.

Announced on October 15, 2024.

_____

Korsak Chairasmisak

Vice Chairman of the Board of Director

and Chairman of Executive Committee

Appendix 1

ITG 001/2567

Information Technology Management and Security Policy

Table of Contents

Table of Contents…….. 10

1. Principles and Rationale…….. 12

2. Objectives…….. 12

3. Scope ……. 13

4. Information Technology Management and Security Policy……. 13

4.1. Information Security Organization and Personal Data Management Policy……... 13

4.1.1. Threat Intelligence Management…… 13

4.1.2. Information Security in Project Management……. 14

4.1.3. Inventory of Information and Other Associated Assets……. 14

4.1.4. Information Classification and Labelling……... 15

4.1.5. Information Transfer……... 15

4.1.6. Access and Authentication Management…… 16

4.1.7. Supplier Management……. 16

4.1.8. Information Security for Use of Cloud Services…… 17

4.1.9. Information Security Incident Management and Personal Data Protection……... 17

4.1.10. Business Continuity Management…… 18

4.1.11. Legal, Statutory, Regulatory and Contractual Requirements……... 19

4.1.12. Protection of Records……... 19

4.1.13. Privacy and Protection of PII…… 20

4.1.14. Independent Review of Information Security……... 20

4.1.15. Documented Operating Procedures…….. 21

4.2. Human Resource Security……... 21

4.2.1. Human Resource Security…….. 21

4.2.2. Remote working…….. 21
4.2.3. Information security event reporting…….. 22
4.3. Physical Controls……. 22
4.3.1. Physical and environmental security…….. 22
4.3.2. Clear desk and clear screen……. 23
4.3.3. Storage media…… 24
4.3.4. Secure disposal or re-use of equipment…….. 24
4.4. Technological controls……. 24
4.4.1. User endpoint devices……. 24
4.4.2. Secure authentication and access control……... 25
4.4.3. Capacity management……. 26
4.4.4. Protection against malware……. 26
4.4.5. Management of technical vulnerabilities…… 26
4.4.6. Configuration management…… 27
4.4.7. Information deletion……... 27
4.4.8. Data masking…….. 28
4.4.9. Data leakage prevention…… 28
4.4.10. Information backup……... 29
4.4.11. Redundancy of information processing facilities……. 29
4.4.12. Logging……. 30
4.4.13. Monitoring activities……. 30
4.4.14. Clock synchronization…….. 31
4.4.15. Installation of software on operational systems…… 31
4.4.16. Networks security management…… 32
4.4.17. Use of cryptography……. 32
4.4.18. Secure development…….. 33
4.4.19. Testing Information…….. 34
4.4.20. Protection of information systems during audit testing…… 34

1. Principles and Rationale

CP All Public Company Limited and its subsidiaries, hereinafter referred to as "the Company," has established the Information Security Management Policy and related guidelines to serve as standards and practices for the Company's information technology systems. This is to ensure that the systems are appropriate, efficient, secure, and continuously improving information security systems. It also aims to prevent problems that may arise from improper use of information systems and threats from various sources, both internal and external, whether intentional or unintentional. This will reduce various damages and maintain the ability to operate efficiently. Furthermore, this policy ensures compliance with the Personal Data Protection Act B.E. 2562 (2019), the Computer Crime Act B.E. 2560 (2017), and other related laws. These operations serve as measures to elevate the Company's information technology security to international standards, referencing the ISO/IEC 27001 and ISO/IEC 27701 international standard frameworks, and utilizing guidelines from Charoen Pokphand Group's information security policies and practices.

2. Objectives

To ensure that the Company's information technology systems are appropriate, efficient, secure, and can operate continuously, and to prevent issues that may arise from improper use of information systems and threats, the Company deems it appropriate to establish an Information Technology Management and Security Policy. This policy defines Standards, Guidelines, Procedures, and Work Instructions to cover information system security and prevent various threats, with the following objectives:

1. To define the direction, principles, and framework of requirements for the Company's information technology security management.
2. To build knowledge and understanding among employees to comply with policies, standards, guidelines, procedures, work instructions, and computer-related laws correctly and appropriately.

3. To enable employees, users, or those connected to the Company's computer systems to use the Company's computer systems correctly and appropriately.
4. To prevent the Company's computer systems and information from being intruded, stolen, destroyed, interfered with, or cyber-stolen in various forms that could cause damage to the Company's business operations.
5. To ensure that information technology security management processes are clear, auditable, and continuously improvable.

3. Scope

This Information Security Management Policy and related guidelines are effective for the Company's information, asset custodians, asset users, committees, executives, employees, temporary staff, and individuals who can access the Company's information. These individuals have a direct responsibility to support, implement, and strictly comply with the policy. Other related users who do not have asset custodianship responsibilities must cooperate in implementing this policy. Violators of this policy will be subject to disciplinary action according to the Company's regulations.

4. The Company has established key Information Technology Management and Security Policies, which comprise:

4.1 Organization of information security and privacy controls

4.1.1. Threat intelligence management

Objective:

1. To recognize and manage threats that may impact the organization, and to implement appropriate prevention and mitigation measures.

Related documents:

1. SCM-PRC-Threat intelligence management

Guidelines:

1. Procedures must be established for collecting and analyzing threat intelligence related to information security to mitigate the impact of threats.

4.1.2. Information security in project management

Objective:

1. To ensure effective management of information security risks related to projects and deliverables.

Related documents:

1. PMP-PRC-Project Management

Guidelines:

1. Project management must integrate information security, including risk management, from the initiation to the conclusion of the project.

4.1.3. Inventory of information and other associated assets

Objective:

1. To identify information and related assets within the organization, as assigned to asset owners, to ensure appropriate control over their use, modification, and disposal.

Related documents:

1. PAM-PRC-Asset Management Procedure
2. ISM-PRC-Acceptable Use of Assets Procedure
3. Data Classification Policy and Practices
4. RSM-PRC-Risk Management Methodology

Guidelines:

1. Procedures must be established for asset management, covering registration, usage, and return of assets.
2. The asset inventory must be reviewed regularly to ensure its accuracy and completeness.
3. Personal data must have a Personal Information (PI) Inventory and a Data Flow process.

4. Risk assessment for the use of information assets and personal data protection must be conducted appropriately.

4.1.4. Information classification and labelling

Objective:

1. To establish principles and guidelines to ensure that the Company's information is managed and protected appropriately in terms of threats to the information, considering its importance to the business.

Related documents:

1. Data Classification Policy and Practices

Guidelines:

1. Adhere to the Data Classification Policy and Practices announced by Data Governance.

4.1.5. Information transfer

Objective:

1. To ensure secure exchange of information with internal and external units.

Related documents:

1. ISM-PRC-Information Exchange Procedure
2. ISM-PRC-Acceptable Use of Assets Procedure

Guidelines:

1. Procedures must be established for information exchange via electronic channels and storage media.
2. Guidelines must be established for users regarding information disclosure through various channels, such as verbal communication and email usage.
3. Confidentiality or non-disclosure agreements must be established.
4. In cases involving the exchange of personal data, a Data Processing Agreement or a Data Sharing Agreement must be established.

4.1.6. Access and authentication management

Objective:

1. To define rules and control access to the unit's information systems, including systems supporting service operations.
2. To protect the unit's information and information technology systems from unauthorized access.
3. To define processes for managing, approving/authorizing, creating, changing, removing, and canceling user accounts and access rights to critical information technology systems of the unit.
4. To uniquely identify individuals and systems that access organizational information and assets, and to assign appropriate access rights.
5. To ensure that authentication information is secure.

Guidelines:

1. Procedures must be established for secure access control to information and assets.
2. Authentication management must be in place, covering the allocation, retention, and cancellation of user accounts.
3. Procedures for managing access rights to information and assets must cover all stages of the user lifecycle, from new user registration, various status changes, to the revocation of user rights.

4.1.7. Supplier management

Objective:

1. To ensure that external service providers maintain security and personal data protection standards consistent with laws, Company policies, and business agreements.

Related documents:

1. SUM-PRC-Supplier Relationship Management
2. SUM-GUI-Third Party IT Practical Guideline
3. RSM-PRC-Risk Management Methodology

4. SUM-PRC-Supplier Relationships Procedure

Guidelines:

1. Procedures must be established for managing external service providers regarding information security, personal data protection, and associated risks related to information products and services.

2. The Company must communicate information security and personal data protection guidelines to external service providers.

3. Regular monitoring must be conducted to ensure external service providers comply with the Company's requirements and conditions.

4. In cases where third parties are hired for system development, agreements on information security and personal data protection must be communicated, and their operations continuously monitored.

4.1.8. Information security for use of cloud services

Objective:

1. To manage information security for the use of cloud services.

Related documents:

1. RDM-PRC-Security Controls for Cloud Procedure

Guidelines:

1. Procedures and policies regarding the use of cloud services must be established and communicated to relevant parties.

4.1.9. Information security incident management

Objective:

1. To enable rapid and efficient response to security breaches and data leakages, and to analyze and improve processes to reduce future occurrences or their consequences.

2. To ensure that the management of security breaches and data leakages complies with legal requirements.

Related documents:

1. ICM-PRC-Incident Management

2. PDA-PRC-Data Incident and Breach Management Procedure

3. Data Breach & Cyber Security Incident Response Plan

4. Data Breach Handling Policy

Guidelines:

1. Procedures for managing security breaches and data leakages must be established, including defining roles, responsibilities, and reporting steps for relevant parties.

2. Criteria for severity levels and responses to security breaches and data leakages must be defined.

3. The results of analysis of security breaches and data leakages must be used for improvement to reduce future occurrences or consequences.

4. In case of security breaches and data leakages, the Data Breach & Cyber Security Incident Response Plan must be followed.

5. In case of personal data breaches, consideration must be given to notifying the Personal Data Protection Committee (PDPC) office and the data subjects in accordance with legal timeframes, referencing the Data Breach Handling Policy.

4.1.10. Business continuity management

Objective:

1. To establish guidelines for business continuity management, enabling the unit to perform critical business processes and/or provide key services to users when emergencies or disasters occur, and to manage an efficient return to normal operation.

Related documents:

1. SCM-PRC-Business Continuity Management

2. SCM-PRC-Service Continuity Management

Guidelines:

1. Procedures for business continuity management must be established for events that

cause business disruption.

2. Plans for business disruption events must be developed, maintained, and tested.

4.1.11. Legal, statutory, regulatory and contractual requirements

Objective:

1. To ensure that operations comply with legal, mandatory, regulatory, contractual requirements, and adopted standards related to information security and personal data protection.

Related documents:

1. ISM-PRC-Acceptable Use of Assets Procedure

2. SUM-CPA-Checklist Legal

Guidelines:

1. Relevant legal, mandatory, regulatory, and contractual requirements related to information security and personal data protection, along with how the Company will comply with these requirements, must be identified.

2. Laws and standards must be continuously monitored for analysis and planning of improvements in accordance with the change management process.

4.1.12. Protection of records

Objective:

1. To ensure that record management complies with legal, mandatory, regulatory, and contractual requirements (records are defined as stored data or events arising from work processes, in both electronic and paper formats, such as data records, sales transaction logs, application logs, etc.).

Related documents:

1. AVM-PRC-Record Control Procedure

Guidelines:

1. Procedures for record management must be established, covering collection, storage, dissemination, destruction, and defining retention periods.

4.1.13. Privacy and protection of PII

Objective:

1. To ensure compliance with legal, mandatory, regulatory, and contractual requirements related to data security in protecting personal data.

Related documents:

1. Data Privacy Policy
2. Personal Information Inventory
3. Data Controller and Data Processor Management
4. Data Protection Impact Assessment

Guidelines:

1. Comply with the Data Privacy Policy and guidelines announced by the Data Protection Office.
2. Guidelines for recording personal data processing activities must be established.
3. Guidelines for data controllers and data processors must be established.
4. Guidelines for Data Protection Impact Assessment must be established.

4.1.14. Independent review of information security

Objective:

1. To ensure that information security management is continuously appropriate, sufficient, and effective.

Related documents:

1. PQA-PRC-Internal Audit Procedure
2. PQA-PRC-Corrective and Preventive Action Procedure

Guidelines:

1. Information security management should be audited by independent parties within the organization.
2. Audit results should be recorded and reported to management.

4.1.15. Documented operating procedures

Objective:

1. To ensure that information security management operations are performed correctly.

Guidelines:

1. Procedures and policies regarding the use of cloud services must be established and communicated to relevant parties.

2. A process for document management must be established A process for document management must be established

4.2 Human resource security

4.2.1. Human resource security

Objective:

1. To define the roles and responsibilities of the human resource management system in the organization, from organizational structure planning, workforce planning, recruitment, selection, performance evaluation, training and development, disciplinary processes, and changes or termination of employment.

Related documents:

1. OPD-PRC-Disciplinary Action Procedure

Guidelines:

1. There must be processes for managing information security and personal data protection in human resources, from organizational structure planning, workforce planning, recruitment, selection, performance evaluation, training and development, disciplinary processes, and changes or termination of employment.

4.2.2. Remote working

Objective:

1. To ensure information security and personal data protection when working remotely.

Related documents:

1. ISM-PRC-Mobile Computing and Teleworking Procedure

Guidelines:

1. There must be processes for managing information security and personal data protection related to mobile device usage, processing devices, and remote working.

4.2.3. Information security event reporting

Objective:

1. To support efficient reporting of information security incidents, data breaches, and data leaks.

Related documents:

1. ICM-PRC-Incident Management
2. PDA-PRC-Data Incident and Breach Management Procedure
3. Data Breach Handling Policy

Guidelines:

1. There must be guidelines for reporting information security incidents, data breaches, and data leaks.

4.3 Physical controls

4.3.1. Physical and environmental security

Objective:

1. To prevent and maintain physical security, unauthorized access, physical damage, including offices, rooms, and facilities.

Related documents:

1. ISM-PRC-Physical and Environment Procedure
2. ISM-POL-Data Center Policy
3. Data Classification Policy and Practices

Guidelines:

1. Secure areas must be defined and used to protect areas with information and other associated assets.
2. Access to various areas, such as transport and loading zones, and other points where

unauthorized persons can enter the premises, must be controlled.

3. Physical security for offices, rooms, and facilities must be designed and implemented in accordance with information data classification levels.

4. Physical access security must be checked for unauthorized access.

5. Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure, must be designed and implemented.

6. Operating guidelines for working in secure areas must be established for relevant personnel, covering all activities occurring in the area.

7. Equipment must be placed securely and protected from physical and environmental threats.

8. Operational procedures must be established to ensure the security of assets when used off-site.

9. Information processing facilities must be protected against power failures and other disruptions, including those affecting supporting utilities.

10. Guidelines for maintaining the security of power cables, communication cables, and other cables supporting information services must be established to prevent loss, damage, theft, or vulnerability, and to prevent organizational disruption.

11. Guidelines for equipment maintenance must be established to ensure its availability, integrity, and confidentiality of information.

4.3.2. Clear desk and clear screen

Objective:

1. To reduce the risk of unauthorized access, loss, and damage to information on desks, display screens, and other accessible locations both during and outside normal working hours.

Related documents:

1. ISM-PRC-Acceptable Use of Assets Procedure

Guidelines:

1. Operating guidelines regarding clear desk and clear screen practices must be established to ensure tidiness and display security.

4.3.3. Storage media

Objective:

1. To ensure that only authorized disclosure, modification, deletion, or destruction of data occurs on information storage media.

Related documents:

1. AVM-PRC-Disposal of Media Procedure
2. Data Classification Policy and Practices

Guidelines:

1. Storage media must be managed from acquisition, usage, transportation, and disposal according to the organization's classification and Company requirements.

4.3.4. Secure disposal or re-use of equipment

Objective:

1. To prevent information leakage from equipment that will be disposed of or reused.

Related documents:

1. AVM-PRC-Disposal of Media Procedure
2. Data Classification Policy and Practices

Guidelines:

1. Procedures must be in place to ensure that data on equipment is securely deleted or destroyed before the equipment is disposed of or reused.

4.4 Technological controls

4.4.1. User endpoint devices

Objective:

1. To protect information from risks associated with the use of user endpoint devices.

Related documents:

1. ISM-PRC-Acceptable Use of Assets Procedure
2. PAM-PRC-Asset Management Procedure

Guidelines:

1. Procedures and user responsibilities must be established regarding the secure use of endpoint devices, personal devices, and wireless connections.

4.4.2. Secure authentication and access control

Objective:

1. To ensure that only authorized users can access information and assets.
2. To prevent unintended or malicious changes to information and protect intellectual property.
3. To ensure that authentication processes are correct and secure when granting access to systems, applications, and various services.

Related documents:

1. ISM-PRC-User Access Management Procedure
2. Data Classification Policy and Practices

Guidelines:

1. Procedures for allocating access rights for privileged access must be more stringent than general access management.
2. Access rights to information and related assets must be restricted according to their confidentiality classification.
3. Access to and modification of source code and related items (e.g., designs, specifications, test plans, and UAT plans) and development tools (e.g., compilers, builders, integration tools, test platforms, and environments) must be strictly controlled.
4. Authentication technologies and procedures must be defined to be appropriate and stringent to reduce the risk of unauthorized access.

4.4.3. Capacity management

Objective:

1. To ensure that various resources (e.g., hardware, software, human resources, offices, and other facilities) have sufficient capacity for business needs.

Related documents:

1. CPM-PRC-Capacity Management

Guidelines:

1. Procedures must be established for monitoring resource usage and adjusting them to align with current capacity and business needs.

4.4.4. Protection against malware

Objective:

1. To securely protect information and other associated assets from malware.

Related documents:

1. ISM-PRC-Acceptable Use of Assets Procedure

Guidelines:

1. Malware prevention procedures and software must be implemented.
2. An appropriate business continuity plan for recovery from malware attacks must be prepared.
3. Malware awareness must be raised appropriately and consistently.

4.4.5. Management of technical vulnerabilities

Objective:

1. To prevent threats arising from the exploitation of technical vulnerabilities in information systems, which could cause damage to the systems and potentially disrupt the organization's business operations.

Related documents:

1. ISM-POL-Vulnerability Management Policy
2. ISM-PRC-Patch Management Procedure

Guidelines:

1. Procedures for appropriate security vulnerability scanning, assessment, and management must be in place.

2. Vulnerability assessments must be conducted at least once a year.

3. Systems connected to public communication networks (Internet facing) must undergo penetration testing before going live (production) or when system changes pose a security risk (e.g., changes in architecture or servers, addition of functions that interact externally, new system integrations).

4. System administrators are responsible for managing, monitoring, and updating patches, especially security patches, in all systems (whether On-Cloud or On-Premise).

4.4.6. Configuration management

Objective:

1. To ensure that hardware, software, services, and networks operate correctly with necessary security configurations and to prevent unauthorized or incorrect configuration changes.

Related documents:

1. CFM-PRC-Configuration Management

Guidelines:

1. Procedures for managing security configurations of hardware, software, services, and networks must be established, documented, implemented, monitored, and reviewed.

2. Standard templates for secure hardware, software, service, and network configurations must be defined.

3. Configurations must be monitored to ensure they are correct and adhere to defined standards.

4.4.7. Information deletion

Objective:

1. To prevent unnecessary information disclosure and comply with legal, regulatory, and

contractual requirements for information deletion.

Related documents:

1. AVM-PRC-Record Control Procedure
2. Data Classification Policy and Practices
3. AVM-PRC-Disposal of Media Procedure
4. Data Controller and Data Processor Management

Guidelines:

1. Procedures for deleting or destroying information stored in information systems, devices, or other storage media must be implemented according to the information's confidentiality classification.
2. A deletion timeframe must be defined when the purpose of information use has ended.
3. In the case of personal data, compliance with relevant personal data deletion laws is required.

4.4.8. Data masking

Objective:

1. To limit the disclosure of critical data, including personal data, and to comply with legal, regulatory, and contractual requirements.

Related documents:

1. Data Classification Policy and Practices
2. Data Controller and Data Processor Management

Guidelines:

1. Procedures must be in place for masking data according to its confidentiality classification, including personal data.

4.4.9. Data leakage prevention

Objective:

1. To detect and prevent unauthorized information disclosure by individuals or systems.

Related documents:

1. ISM-PRC-Information Exchange Procedure

2. Data Breach Handling Policy

Guidelines:

1. Procedures for preventing and monitoring assets against data leakage risks must be established.

4.4.10. Information backup

Objective:

1. To enable data recovery in case of system or data loss.

Related documents:

1. AVM-PRC-Information Backup and Restore Procedure

2. Data Classification Policy and Practices

Guidelines:

1. Procedures for data backup, data recovery, and regular data recovery testing must be in place.

4.4.11. Redundancy of information processing facilities

Objective:

1. To ensure that systems and infrastructure support continuous operations as per business requirement.

Related documents:

1. SCM-PRC-Business Continuity Management

2. SCM-PRC-Service Continuity Management

Guidelines:

1. The Company must design its system architecture and infrastructure to support business continuity requirements, based on ICT readiness for business criteria.

4.4.12. Logging

Objective:

1. To record events, create evidence, ensure log integrity, prevent unauthorized access, for identifying information security and personal data protection incidents, and to serve as evidence supporting investigations.

Related documents:

1. AVM-PRC-Logging and Monitoring System Use Procedure
2. PDA-PRC-Data Incident and Breach Management Procedure

Guidelines:

1. Guidelines for event logging must be established (e.g., Event Log, Access Log, User Activity Log, Authentication Log, Transaction Log).
2. Guidelines for maintaining the security and personal data protection of event logs must be established.
3. Guidelines for regular review and analysis of abnormal data from event logs must be in place to manage security according to Incident Management procedures.

4.4.13. Monitoring activities

Objective:

1. To detect abnormal behavior and potential information security and personal data protection incidents.

Related documents:

1. AVM-PRC-Logging and Monitoring System Use Procedure
2. ICM-PRC-Incident Management
3. PDA-PRC-Data Incident and Breach Management Procedure

Guidelines:

1. The scope and level of monitoring for networks, systems, and applications must be defined according to business needs, security requirements, laws, and relevant regulations.

2. Monitoring activities must be recorded.

3. Thresholds and alerts must be defined for monitoring abnormal behavior.

4.4.14. Clock synchronization

Objective:

1. To establish correlation and analyze security-related events and other recorded data, including supporting information security investigations.

Guidelines:

1. All computers in the Company must be configured to synchronize their time with a time server (e.g., time.navy.mi.th.or.th or time2.navy.mi.th from the Hydrographic Department, Royal Thai Navy, serving as Stratum 1 time data, or according to Active Directory) using Network Time Protocol (NTP).

2. All devices must have their time synchronized with the standard time.

4.4.15. Installation of software on operational systems

Objective:

1. To ensure the integrity of the operating system and prevent the exploitation of technical vulnerabilities.

2. To ensure that the use of utility programs does not harm the control of systems and applications for information security.

Related documents:

1. IT-STD-Program standards for use in company operations

2. ISM-PRC-User Access Management Procedure

3. ISM-PRC-Acceptable Use of Assets Procedure

Guidelines:

1. Procedures for managing changes and securely installing software and libraries on operational systems must be in place, ensuring they are not End of Support.

2. If privileged utility programs are required, it must be verified that these programs are not harmful and do not negatively impact the operating system and applications.

3. Access rights and usage logs for users of privileged utility programs must be controlled.

4.4.16. Networks security management

Objective:

1. To ensure the security of information, resources, and activities within the network, preventing attacks and unauthorized resource access.

Related documents:

1. ISM-PRC-Network Security Procedure
2. ISM-PRC-User Access Management Procedure

Guidelines:

1. Network security guidelines must be established.
2. The scope for each network type must be defined.
3. Appropriate web filtering guidelines must be established.

4.4.17. Use of cryptography

Objective:

1. To ensure appropriate and effective use of cryptography to protect the confidentiality, integrity, or completeness of information, considering business requirements and relevant legal, mandatory, regulatory, and contractual requirements related to cryptography.

Related documents:

1. ISM-PRC-Cryptography Control Procedure
2. Data Classification Policy and Practices

Guidelines:

1. Encryption standards must be defined based on confidentiality classification.
2. Key management standards must be defined.

4.4.18. Secure development

Objective:

1. To control the development and changes of information systems and software to be efficient and secure from the design process, development, testing, and operational planning, leading to an efficient implementation process and reducing the risk of damage to core information systems.

Related documents:

1. RDM-PRC-Information System and Software Development
2. TSM-FRM-Privacy by Design Guideline for IT
3. CHM-PRC-Change Management Procedure
4. SUM-GUI-Third Party IT Practical Guideline

Guidelines:

1. Procedures for secure system development and personal data protection must be established.
2. If the system processes personal data, it must comply with the Privacy by Design Guideline for IT as defined by the Company.
3. System security requirements must be defined.
4. Security engineering principles must be defined and applied to system design and development.
5. A process must be in place to ensure secure coding of programs, both before, during, and after coding.
6. Security testing processes must be in place for new systems or modified systems.
7. In cases where third parties are hired for system development, security agreements must be communicated, and their operations continuously monitored.
8. Development, Test, and Production environments must be separated.
9. A change management process must be established.

4.4.19. Testing Information

Objective:

1. To ensure that testing processes are appropriately protected.

Related documents:

1. RDM-PRC-Information System and Software Development

Guidelines:

1. Procedures for security management during testing must be established.

2. Users must avoid using real data. If using real personal data is necessary, a risk assessment must be conducted, protection measures found to prevent data leakage, used for the shortest possible time, and data must be deleted immediately after testing is completed.

4.4.20. Protection of information systems during audit testing

Objective:

1. To ensure that information and information systems are appropriately protected during audits.

Related documents:

1. PQA-PRC-Internal Audit Procedure

Guidelines:

1. A process for managing security during audits must be established.