



## Information Security Management System (ISMS) Policy

Document no.	ISMS-PC-01-MIS
Effective date	22 April 2024
Confidentiality level	Internal
Document owner	Information technology department
Enforcement on	Personnel
Approver	ISMS Management Committee



# ORIGINAL ISMS

## Document approval

### Document owner

Name

Mr. Chawalit Suttisumton

Position

Manager

Date

22 April 2024

Signature



(ISMS Working Committee)

### Document reviewer

Name

Miss Preeyaporn Sangehot

Position

Lead Officer

Date

22 April 2024

Signature



(Document Control Officer)

### Document approver

Name

Mr. HSIN-WANG

Position

Chief Financial Officer

Date

22 April 2024


Signature



(ISMS Management  
Committee)

## Table of Contents

	Page
1. Introduction .....	1
2. Policy elements .....	1
3. Enforcement and Penalties .....	2
4. ISMS Policy .....	2
5. Relevant documents .....	20
6. Document to be records.....	21

	Title: Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

ORIGINAL ISMS

## 1. Introduction

Apex Circuit (Thailand) Co., Ltd. (“Company”) considers on the significance of bringing information technology to help increasing the potential of the company’s operation in order to create the systematic management procedures with regulations and steps to reduce the redundancy and to respond to the needs of service users and business continuity.

The company foresees that bringing information technology into the operation required establishing an information security management system policy as guidelines to develop the compliance to the company’s strategy and vision, as well as the laws, regulations, and any relevant universal standard and changes in the current information technology. Therefore, information technology services could be effectively and efficiently done with the security and good information technology framework. The related parties would have confidence in the company’s information system services.

## 2. Policy Elements

Section 1 Information Security Responsibilities

Section 2 Administrator Responsibilities

Section 3 Mobile Device

Section 4 Teleworking

Section 5 Human Resource Security

Section 6 Password

Section 7 Personal Computer/Notebook

Section 8 Software Computer

Section 9 Internet and Network Service

Section 10 E-mail Service

Section 11 Online Social Networking

Section 12 Publish Information on Website

Section 13 Information Protection

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

**ORIGINAL ISMS**

- Section 14 Physical and Environment Security
- Section 15 Cryptography
- Section 16 Malware Protection
- Section 17 Intellectual Property
- Section 18 Information Sharing
- Section 19 Information Security Reporting
- Section 20 Business Continuity Management
- Section 21 Cyber Security Management
- Section 22 Cloud Computing Security
- Section 23 Information Security Project Management
- Section 24 Access Control
- Section 25 Communication Security
- Section 26 Risk Management
- Section 27 System Acquisition, Development and Maintenance
- Section 28 Taking computers allocated by the Company out of the area


### 3. Enforcement and Penalties

This information security management system policy is effective since the date of announcement to the information system users of Apex Circuit (Thailand) Co., Ltd. under all scope of request for certification without exception. The violators will be guilty and subject to disciplinary actions based on the regulations set forth by the company.

### 4. Policy

#### 4.1 Section 1 Information Security Responsibilities


- (1) Employees shall responsible to preserve the security of an information system according to the information security requirements under this document.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

- (2) Supervisors at all levels shall responsible to govern their subordinates to practice strictly on the requirements under this document.
- (3) Employees who breach the laws such as Computer Crime Act B.E. 2550 (2007) and Computer Crime Act (No. 2) B.E. 2560 (2017) or Cyber Security Act B.E. 2562 (2019), Personal Data Protection Act B.E. 2562 (2019) and other laws, plus, violations of information security of Apex Circuit (Thailand) Co., Ltd. from the fact of an act of improper intent shall be considered as a disciplinary offence.

#### 4.2 Section 2 Administrator Responsibilities

- (1) User account and password are required to control and look after information technology system. If necessary or with some limitation, the control on usage should be in form of written notice on the assignment.
- (2) Computer system needs good care and improvement on the use based on skills and monitoring on the computers, computer equipment, computer network, and computer data used should be in accordance to this policy.
- (3) Crucial business data, Operating System, Application System and Source Code should be completely backed up and prompted for availability. Moreover, the data backup media should be stored in external place by the practice should refer to document *ISMS-PD-06-MIS\_ Backup and Restore Procedure*
- (4) Setting access control to control data use based on the right of users as proper.
- (5) One shall not wrongly access into personal information including business data or act in a way to violate the laws.
- (6) Practice on document *ISMS-PD-04-MIS\_Change Control Procedure control* when there is the need to change equipment in computer system, computer, or computer system equipment.
- (7) To control, store, and prevent computer data or information based on document *ISMS-PD-05-MIS\_ Information Classification, Labelling and Handling Procedure*.


	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

- (8) Preparing manual, guidelines, or any necessary things to control or operate on computer, computer equipment, computer data, or information by they should be made in written forms, or it can be in form of electronics or printed media. Thus, types or amounts of such manual or operation procedures should be in accordance with document *ISMS-PD-05-MIS* Information Classification, Labelling and Handling Procedure.
- (9) Conducting data verification, documents, or reports and correction as necessary before recording data or brining out from work system of Apex Circuit (Thailand) Co., Ltd.

#### 4.3 Section 3 Mobile Device

- (1) Mobile devices such as Laptop Computer, Smartphone, Tablet, etc.
- (2) Recording media such as CD- ROM, DVD-ROM and Removable Media such as External Hard Disk, Thumb Drive, CD- ROM, DVD-ROM, etc.
- (3) Employees who need to use mobile device or recording media which are the assets of Apex Circuit (Thailand) Co., Ltd. shall request for the approval to borrow such device. It must be approved before bringing to use and after finished the use, the device must be returned to Apex Circuit (Thailand) Co., Ltd.
- (4) In case the employees bring personal mobile devices that do not belong to Apex Circuit (Thailand) Co., Ltd. to use in the company, it can be divided in two cases as follows:
  - a) Personal mobile device that has been used regularly for the operation and can access into information system of Apex Circuit (Thailand) Co., Ltd.
    - Required to register to access into network and information system service of Apex Circuit (Thailand) Co., Ltd. and it shall pass the authentication every time before accessing to services.



	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

**ORIGINAL ISMS**

- Acquired the right to access into the particular system related to one own operation required for the approval from the authority.
- Setting password control as defined in Section 6 on password used in this policy document.

b) Personal mobile device for temporary use should be

- Registered to request for wireless network service from Apex Circuit (Thailand) Co., Ltd. and it must be authenticated every time before accessing to use.
- Unable to use any resources within an information technology system of Apex Circuit (Thailand) Co., Ltd. IT officer only allow for personal mobile device usage on an internet system.
- Set for mobile device password.

(5) To set for the safe network system and access monitoring system.


(6) Data collection for the operation in Apex Circuit (Thailand) Co., Ltd. via mobile device or recording media either as the assets of Apex Circuit (Thailand) Co., Ltd., or personal assets must be strictly and securely protected either in Apex Circuit (Thailand) Co., Ltd. or in public places.

(7) Be careful and avoid leaving mobile device, or recording media in public place, or a place where it can be easily found and reached to.

(8) Apex Circuit (Thailand) Co., Ltd. preserves the right to check on mobile device, or recording media either the assets of Apex Circuit (Thailand) Co., Ltd. or personal assets.

#### 4.4 Section 4 Teleworking

(1) Employees shall not give user account for the use of other and one must responsible for the damages that may occur.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0


- (2) Employees should register for the use based on document *ISMS-PD-14-MIS\_Teleworking Procedure*. Apex Circuit (Thailand) Co., Ltd. preserves the right to suspend the use of VPN system if there is a doubt on the unsafety of the network.
- (3) Using VPN system requires secure password based on the universal standard such as SSL, etc.

#### 4.5 Section 5 Human Resource Security

- (1) Having a proper personnel screening to check on the background of the applicants that conform to the laws, rules, regulations, and relevant ethics. It also needs to process on the level that suited to their position and duties.
- (2) The operation agreement should be made as required by Apex Circuit (Thailand) Co., Ltd. in an employment agreement.
- (3) Arranging for training to provide knowledge and forming awareness and training on information security.
- (4) There shall be the procedure for termination of the employment or changes of duties, as well as right cancellation for the access into information technology system and Apex Circuit (Thailand) Co., Ltd. network, as well as return of assets when returning all the assets and end of duties.

#### 4.6 Section 6 Password

- (1) Employees need to use their own password to authenticate themselves for the access into the operation in an information system based on the assigned rights only.
- (2) Employees who received password for the first time should change new password immediately for self-secret. In case that password has been revealed, employees have to change to new password immediately.


	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

**ORIGINAL ISMS**

- (3) If users found any doubtful reason that password is used by the others, he/she should change password and inform to “the administrator” immediately.
- (4) Password should have at least 8 characters consisting of alphabet, number, or symbols that can be hardly guessed or based on top capacity of the system.
- (5) Do not set password from one own name or surname, or people in family or those with close relationship; or vocabulary in dictionary.
- (6) Setting to change password for every 6 months for general users and every 3 months for technical operators in any systems. Thus, it shall be considered on the impact and severity toward information, image, and reputation of Apex Circuit (Thailand) Co., Ltd.
- (7) Do not reveal password to the others.
- (8) Do not write password in a paper or post it on computer or desk area.
- (9) Do not bring old password to use for 3 times or 4 times including the present.

#### 4.7 Section 7 Personal Computer/Notebook


- (1) Looking after personal computer/notebook to be in good condition and only use computer in normal way. It is not allowed to adjust or reduce any equipment of such computer.
- (2) Do not install or remove computer program that installed or set to use. Software installation shall comply with document *ISMS-PD-15-MIS\_ Installation of Software Procedure*
- (3) Do not install and use FTP (File Transfer Protocol) program for data movement.
- (4) If the personal computer/notebook are found to have defect, damage, or lost, after the investigation and found that the item was used with insufficient care, one shall responsible for such damage and lost.
- (5) It is not allowed to bring personal computer/notebook to use for other purposes apart from the tasks under assigned responsibilities.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

- (6) Deleting or having measure for the key data protection (such as data encryption for confidential data or data for only internal use) in pc computer/notebook before sending to fix.
- (7) Data backup in pc computer/notebook that have been used regularly to help protecting the loss of information from many cases such as damaged hard disk, the power surge that may cause hard disk crashes, or else.
- (8) Do not use pc computer/notebook in a way that would lead to damage of the others, the company or breach of any laws or good morals as follows:
- Wrongly access into data, network, or work systems without permission
  - To interrupt or disrupt the network or work systems
  - Intercepting the information of others.
  - Smuggling to decode password
  - Unlawful or unauthorized tampering or alteration of information
  - Improper distribution of images, message, or sound
  - Any illegal acts with an intention that deviated from the normal use behavior.
- (9) Be careful and preserve notebook when using it outside the office to prevent loss and do not leave notebook without people.
- (10) Do not allow the other to use notebook of Apex Circuit (Thailand) Co., Ltd.
- (11) Authentication is required before accessing to use pc computer/notebook every time.
- (12) Checking to set the screen saver in order for the notebook to lock screen automatically after the computer has not been used for more than 15 minutes.

#### 4.8 Section 8 Software Computer

- (1) Employees shall use computer software based on the standard set by Apex Circuit (Thailand) Co., Ltd.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

**ORIGINAL ISMS**

- (2) Employees are not allowed to bring unauthorized software to use on the computer of Apex Circuit (Thailand) Co., Ltd. If there is a filed lawsuit from the victim, such employee has to responsible for all the damages occurred.
- (3) Employees are not allowed to use computer device of Apex Circuit (Thailand) Co., Ltd. to produce, own, or sell improper or illegal software.
- (4) Apex Circuit (Thailand) Co., Ltd. preserves for the right to investigate on data in employees' computer, if there is a doubtful reason that employees may act in a way that may cause damages to Apex Circuit (Thailand) Co., Ltd.

#### 4.9 Section 9 Internet and Network Service

- (1) Using for the operation under the mission of the unit or self-responsibility
- (2) Do not use internet and network service of Apex Circuit (Thailand) Co., Ltd. for
  - The acts of non-conformity to the Computer crime Act.
  - Obscene; websites showing anti-national, religious, monarchical content; websites that pose a threat to society and undermine national security, etc.
  - Playing games, watching movies, or listening to the songs during work hours.
  - Chatting on internet network during work hours.
  - Downloading piracy data or program which is an infringement of the rights or intellectual property rights of others
  - Being a channel to invade into the system of others.

#### 4.10 Section 10 E-mail Service


- (1) Using e-mail to operate under the mission of unit or self- responsibility as assigned.
- (2) Carefully use and checking on the recipient's e-mail address to prevent wrongly forwarding of major information and causes data leakage.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

- (3) Defining the name of sender, position, and contact in all sending e-mail for the reply.
- (4) Using polite word in an e-mail
- (5) Limiting data forwarding via e-mail to the recipients or the group of recipients as for those necessary to acknowledge the information in an e-mail.
- (6) Backup e-mail data regularly based on necessity.
- (7) In contacting for the assigned tasks or responsibilities with the internal and external unit, do not use other e-mail addresses apart from that set by Apex Circuit (Thailand) Co., Ltd.
- (8) It is not allowed to access into the e-mail of others without permission.
- (9) It is not allowed to register an e-mail address of Apex Circuit (Thailand) Co., Ltd. on other websites that are not related to the work of oneself.
- (10) It is not allowed to send Spam Mail.
- (11) It is not allowed to send Chain Letter
- (12) It is not allowed to send an e-mail that violates the laws, the rights and intellectual property of the others.
- (13) It is not allowed to send an e-mail with malicious program to the other with intention.
- (14) Do not create fake or use e-mail of the others.
- (15) Do not send or receive an e-mail instead of the others without permission.

#### 4.11 Section 11 Online Social Networking

- (1) Employees shall not use online social networking that causes damage for Apex Circuit (Thailand) Co., Ltd., rights infringement, illegal, immoral, seeking for the benefits or allowing the other to take business advantages.
- (2) Employees shall not chat or send confidential information of Apex Circuit (Thailand) Co., Ltd. through online social networking.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0


- (3) Employees shall not use e-mail of Apex Circuit (Thailand) Co., Ltd. to register to use online social networking.

#### 4.12 Section 12 Publish Information on Website

- (1) Data verification and checking for the appropriateness before publishing on Apex Circuit (Thailand) Co., Ltd.'s website.
- (2) Supervisor of the staff who responsible on the task shall recheck on the appropriateness and verify the content before publishing them on the website.
- (3) After publishing information online, staff shall always monitor the website in order to see if there are any changes without permission.

#### 4.13 Section 13 Information Protection

- (1) Employees shall not breach the personal information of the others.
- (2) Employees shall not access to the information of others, as well as business information without permission from the information owner.
- (3) Employees shall not print or copy confidential data of Apex Circuit (Thailand) Co., Ltd. and the others except there is a permission from data owners.
- (4) Employees shall set the confidential level of electronic information and practice according to document *ISMS-PD-05-MIS\_Information Classification, Labelling and Handling Procedure*, plus do not reveal confidential information to the irrelevant person.
- (5) Employees shall store data and information related to the works of Apex Circuit (Thailand) Co., Ltd. within the cabinet or the storage place when it is no necessity for use and they shall be protected from any disclosure from negligence.
- (6) Employees shall verify and review the rights of electronic data used together in the computer network of Apex Circuit (Thailand) Co., Ltd.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

**ORIGINAL ISMS**

#### 4.14 Section 14 Physical and Environment Security

- (1) There shall be security protection in the area of data processing. It requires to have appropriate access control that sets only for those with permission to have the right to enter into the area via practicing according to *ISMS-PD-19-MIS\_Physical and Environmental Security Procedure*.
- (2) Access control is required in the delivery area with all equipment check, thus, the area shall be separated from data processing area with devices in order to avoid unauthorized access.
- (3) Equipment shall be protected against power failure and other interruptions caused by the failure of systems and supporting equipment.
- (4) Signal cable should be stored in an orderly manner to prevent damage and to prepare or improve the label of equipment and cables in the computer center to be accurate and complete.
- (5) Inspecting the devices containing the storage media to ensure that sensitive data and licensed software are securely terminated, deleted or overwritten before disposing the device or reusing it.
- (6) Having securely deletion or other management methods for storage media that stores important data that is not necessary to use.

#### 4.15 Section 15 Cryptography

- (1) Significant data of Apex Circuit (Thailand) Co., Ltd. required to have the universal data encryption measure that conform to the agreement, related regulations and laws.
- (2) Apex Circuit (Thailand) Co., Ltd. shall set for the approach of key Management Life Cycle according to document *ISMS-PD-12-MIS\_ Cryptography Management Procedure*



	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

**ORIGINAL ISMS**

#### 4.16 Section 16 Malware Protection

- (1) Employees shall not adjust or cancel the work of anti-virus program that installed in pc computer/notebook.
- (2) Employees shall not download any data or software from the improper websites.
- (3) Employees function to follow up the news related to virus warning and data safety from the public relations of Apex Circuit (Thailand) Co., Ltd.
- (4) Checking virus protection program in the using computer to be in normal status and always update the information. If found abnormal function, it shall be immediately reported to the responsible unit for the immediate correction.
- (5) Checking computer data via anti-virus program (only installed in that computer) to eliminate virus at least once a week.

#### 4.17 Section 17 Intellectual Property


- (1) Following the condition or what required by other software and other intellectual property that Apex Circuit (Thailand) Co., Ltd. or users are using or owning.
- (2) Do not copy, change, or revise on any intellectual property into other forms that breached the using conditions or agreement.
- (3) Do not copy all or some part of the books, journals, reports, or other document that will violate the conditions of the intellectual property owner.

#### 4.18 Section 18 Information Sharing

- (1) Information exchange between Apex Circuit (Thailand) Co., Ltd. and the third party shall be done in secure way and conform to the levels of information management.

#### 4.19 Section 19 Information Security Reporting

- (1) When finding security incident, it shall be reported to those who can help as soon as possible.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

- (2) Coordinating and cooperating with those who help managing on such incident.

#### 4.20 Section 20 Business Continuity Management


- (1) Employees shall cooperate to rehears on business continuity plan as stated in the document of *ISMS-PD-11-MIS\_ Business Continuity Management Procedure* or other plans related to information security management system.
- (2) Rehearsing BCP plan at least once a year.

#### 4.21 Section 21 Cyber Security Management

- (1) There should be a preparing measure for a Cyber security Incident.
- (2) There should be a preparing measure to respond for cyber security incident.
- (3) There should be a follow up on the cyber security incident.

#### 4.22 Section 22 Cloud Computing Security

- (1) Setting for the strategic and policy of Cloud Computing service for the third party service provider.
- (2) There shall be risk management guideline for the use of Cloud Computing service
- (3) It requires for outsourcing Cloud computing service provider management
- (4) It requires to preserve the security and confidentiality of the work system and data using Cloud Computing services.
- (5) It requires processing to ensure that work system and data from Cloud Computing service are credible and valid.
- (6) It requires processing to ensure on the availability of Cloud Computing services related to the protection of personal data that covered on the users of Apex Circuit (Thailand) Co., Ltd.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

**ORIGINAL ISMS**

#### 4.23 Section 23 Information Security Project Management


- (1) Division management shall set for the risk control, project follow up, and overall project assessment both the internal protect and procured projects from external agencies.
- (2) The project owner should set for the agreement and needs of information security related to the ISMS policy and information security practices or any relevant rules and regulations of the company that stated in the contract or project agreement.
- (3) The project owner shall set for the penalties when the operators do not comply with ISMS policy and information security best practices, or any relevant rules and regulations.

#### 4.24 Section 24 Access Control

- (1) Apex Circuit (Thailand) Co., Ltd. shall set for the management approach on the registration and cancellation of the users' right in written forms and always update to the present version. In addition, this should be communicated to those users outside the company to acknowledge and practice accordingly.
- (2) Apex Circuit (Thailand) Co., Ltd. and the data owner shall assign or set for the user right to access into data or information system based on their responsibility.
- (3) Apex Circuit (Thailand) Co., Ltd. shall arrange for password management for high privilege users.
- (4) Apex Circuit (Thailand) Co., Ltd. shall set for the confidential data management approach for user authentication.

#### 4.25 Section 25 Communication Security

- (1) The administrators must control and govern on computer network control management to prevent threats and to maintain the security of information systems and applications running on computer networks including the exchanging information on the network.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0


- (2) The administrators must control to define the security qualifications, levels of service, and needs for the whole network management into the network services contract or agreement either on internal or external service.
- (3) Apex Circuit (Thailand) Co., Ltd. shall set for the appropriate separation of computer networks by considering on the users' need to access into the network, information security impact, and level of confidential data on such network.

#### 4.26 Section 26 Risk Management

- (4) The company will manage and seek for the opportunity under the acceptable risk level in order to achieve the operation objectives and company's goals.
- (5) Top executive management shall set for the company strategic in conformance to the acceptable risk level.
  - There shall be the follow up on risk management in order to ensure that the company keeps properly manage on risks. Risk management framework shall refer to document *ISMS-PD-03-MIS\_ Risk Management Procedure*

#### 4.27 Section 27 System Acquisition, Development and Maintenance)

- (1) System administrators and system developers shall prepare for the procedures for controlling on changes management of information systems or work systems. Thus, the procedures shall include the followings.
  - Potential impact from changes
  - Condition to ask for the approval on the information system or work system revision or development.
  - The operation process in case there is an emergency changes on the system, it requires to record the needs and asking for the approval from the division authority every time.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0


**ORIGINAL ISMS**

- Planning for information system or work system changes.
  - Storing the previous version of program to use or having the Fall-Back procedure in case there is an error on the system and cannot be used.
  - Testing on information system and work system changes.
  - Communicating with the relevant person to know and to operate correctly.
- (2) System administrator shall follow up and check on the use of information system after changed in order to check on any impacts from change on the system works and no impact on information security.
  - (3) System administrator shall control and install software on the information system that provides real service by proceeding with best practice to control on change management in the information system as required.
  - (4) System administrators and system developers shall limit for any changes on the using Software Package by only allow for the necessary change and strictly control on every change.
  - (5) System administrators and system developers shall control and set for the least requirements for the information system development and information security control on new information system, or the old system improvement into the contract and agreement either in the internal project or the procured projects that processed by the outsourcing agency.
  - (6) System administrators and system developers shall always check on any data to receive into the application to ensure that data are accurate and being in proper form.
  - (7) System administrators and system developers shall control and check on the application works or seek for any data errors that result from work or wrong processing.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

**ORIGINAL ISMS**

- (8) System administrators and system developers shall control to have the least limitation to preserve on the authenticity and integrity of the application data. Including to define and properly practice on the protection approach.
- (9) System administrators and system developers shall control to check on any data that resulted from the application processing to ensure the correct and proper information from data processing.
- (10) System administrators and system developers shall set to use of techniques related to encryption as follows:
  - Data categorizing and communication that needed to be encrypted such as password, etc.
  - System administrators shall set to use the program that can encrypt the data for the personnel to use as the same standard. The program shall properly function to encrypt the data when connecting from the company network to the server computer or other network devices of the company.
  - System administrators shall set to use the program that can encrypt the data for the personnel to use as the same standard. The program shall properly function to encrypt the data when connecting from the network outside the company into the company's network.
- (11) System administrators shall set for the guideline of data encryption by key management to support for the use of encryption techniques. By setting for the control, monitoring, and supervising to cover all the cycle that key encryption is used.
- (12) System administrators and system developers shall limit the access into the Source Code of work system.
- (13) System administrators and system developers shall control on the review of the work by the significant program in case of any changes in computer operation

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

**ORIGINAL ISMS**

system. It shall be controlled and having test to ensure that change will not affect on information system security and information system service.

(14) System administrators shall always check on the relevant data to the technical vulnerability to know about threats and risks, as well as seeking for the proper protection and solution for that vulnerability.

(15) System administrators and system developers shall hold on the Secure System Engineering Principles and apply it in the system development.

(16) System administrators and system developers shall control on the system development environment and integrity to be secured. It shall protect the system data that rise during the development, data sending and receiving, data backup and access control to the system.


(17) System administrators and system developers shall test on the information security of new developing system's work function, or in every time of changes.

The test shall consists of following.

- Unit Testing
- Integration Testing
- Test on connection or communication between software and other system testing
- User Acceptance Test: UAT

(18) In case of hiring external outsourcing to develop the system, system administrators and system developers shall control on the software development project by such outsourcing agency as follows:

- Governing, controlling, following up, and checking the work of outsource, as well as subcontracting system development to operate in accordance with the company's regulations on a regular basis.

	<b>Title:</b> Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

- To establish the intellectual property ownership for the source code that developed by outsource in the employment contract.
- To preserve on the right to check on the quality and validity of developed software by outsource in the employment contract.
- To set for the malicious program checking in work system or other software before the installation.

(19) After the outsourcing agency submitted the developed software, system administrator and developer shall change all the default passwords immediately.

#### 4.28 Section 28 Taking computers allocated by the Company out of the area.


In the event that employees bring computers allocated by the company and brought back to use at home The following instructions must be followed:

- (1) Employees must maintain computers allocated by the company as if they were their own property.
- (2) Employees must not place computers allocated by the company in unsafe areas, such as in vehicles where property can be seen.
- (3) Employees must not bring the company's computer for others to use.

#### 5. Relevant documents

- ISMS-PD-03-MIS\_Risk Management Procedure
- ISMS-PD-04-MIS\_Change Control Procedure
- ISMS-PD-05-MIS\_Information Classification, Labelling and Handling Procedure
- ISMS-PD-06-MIS\_Backup and Restore Procedure
- ISMS-PD-11-MIS\_Business Continuity Management Procedure
- ISMS-PD-12-MIS\_Cryptography Management Procedure
- ISMS-PD-14-MIS\_Teleworking Procedure
- ISMS-PD-15-MIS\_Installation of Software Procedure



	Title: Information Security Management System Policy (ISMS Policy)	Confidentiality level: Internal
		Version: 2.0

ORIGINAL ISMS

- ISMS-PD-19-MIS\_Physical and Environmental Security Procedure

6. Document to be records

-