Advance Info Service
Public Company Limited

414 AIS Tower
Phaholyothin Rd., Samsen Nai,
Phayathai, Bangkok 10400

Cyber Security Standard for Third Party (Translation)

AIS Group

Version: 1.0

Document Owner: Cyber Security

Last Updated: 20 June 2024

Document Control

Version History

The following table records all the revisions made to this document:

Version	Date	Created by	Details	Reviewed by	Approved by
1.0	20 June 2024	Cyber Security	Initial release	H-DPO, H-PATH, H-CS	CIO

Table of Contents

Cyber Security Standard for Third Party

1. Introduction

1.1 Objectives

1) This standard maintains cyber security for current third parties who can connect or access the company's information system, including third party who is provided service to the company’s customer under the company’s name.
2) To prevent the company's computer and information systems from being invaded, stolen, destroyed, interfered or from possible cybercrime that may cause damage to the company's business operations when using third parties' service, connection, or access.
3) To reduce the risk to the security of the company's information when using third parties' services, connections, or access.

1.2 Scope

This standard covers cyber security, information system security, and security of the company's information when using third parties' services, connections, or access to information related to the company's information technology system.

1.3 Definitions

1) **"Company"** refers to Advanced Info Service Public Company Limited and any other subsidiaries company in the AIS Group.
2) **"Third Party"** refers to Personnel or external party that conducts business or provides services may be granted access to the company's information and information processing equipment. The term also includes personnel or external parties that are granted rights to access the company's clients' data as below:
    - Business Partner
    - Outsource
    - Supplier
    - Service Provider
    - Consultant
    - External Auditor
3) **"Sensitive Information or Confidential Information"** refers to the information essential to the company's business operations or data bound by legal requirements, business ethics, or contracts that the company may not disclose to other persons or use for purposes besides the company's business objectives. Leakage of important or confidential information may disrupt the company's business

operations, reduce work efficiency, or cause reputation damage. The data are divided into six domains: Customer Data, Employee Data, Partner Data, Financial Data, Network Data, and Strategic Data.

4) **"Removable Media"** refers to a portable device that can record and store data, such as a Thumb drive, CD, Diskette, iPod, Electronic Organizer, PDA, or Pocket PC.

5) **"Susceptible System"** refers to work systems are considered susceptible or critical work systems that must be in a separate environment.

6) **"Change Control"** refers to the process of reviewing, testing, and authorizing changes and the impacts before the actual operations on computers or information systems.

7) **" Major Change"** refers to a change that affects the service providing or may have severe consequences to assets and work systems, such as service interruptions for an extended period, the loss of property or life, or disasters. Still, the event may not occur immediately and does not require an urgent fix, but take some time to consider the impact and proceed with the corrections carefully.

8) **" Log file"** refers to information related to computer system communications that indicate the origin, destination, route, time, date, quantity, duration, type of service, or anything related to the communication of such computer system.

9) **"Security by Design"** refers to an approach to computer systems or applications development that seeks to make them secure from the beginning. The development will emphasize preventing cyber threats from the start of the system design process and considering various security principles, such as confidentiality, integrity, and availability, for example, encryption and multi-factor authentication.

10) **"Security by Default"** refers to guidelines for setting up a computer system or application to be secure. The guideline focuses on protecting against the risks of cyber threats without requiring users to adjust additional security settings, for example, by turning off unnecessary applications and setting a strong password.

1.4 Exceptions

The third party must inform the company's supervisor when unable to apply this standard to proceed with the company's risk management process.

1.5 Consequence for Non-Compliance

Suppose the external party violates this standard, policies, guidelines, and company regulations, which may cause damage to the company. The company reserves the right to consider penalties according to the service contract.

2. Roles and Responsibilities

2.1 Company's Project Manager

The project manager shall coordinate with a third party and ensure the company's policy and current standards are implemented.

2.2 Third Party

1) The third party shall learn, understand, and strictly follow the company's policies, standards, operating procedures, methods, guidelines, recommendations, and processes related to cyber security.
2) Cooperate fully with the company to protect the company's computer systems and information.
3) Notify the company immediately when seeing incorrect or inappropriate practices or witness intrusion, theft, destruction, or interference with work or espionage that may cause damage to the company.

3. Cyber Security Standard

The Third Party shall follow the security practices to achieve the following objectives:

- **Confidentiality** – Protecting the confidentiality of information. Prevents access and disclosure of information by unauthorized persons and protects personal or company-proprietary information.
- **Integrity** – Ensuring that the company's information is not altered, modified, or destroyed by any unauthorized person.
- **Availability** – Ensuring authorized users can access information and services quickly and reliably.

3.1 Cyber Security Risk Management

1) Third party must conduct a cyber security risk assessment at least once a year, or whenever there is a significant change.
2) In cases where a risk assessment identifies a risk that exceeds the acceptable level, the external party must develop a risk mitigation plan or risk treatment plan and submit it to the company.
3) The company's responsible departments must cooperate in conducting audits and assessing cyber security risks that may occur with the company's computer system.
4) Any products or services of the external parties that have access to the company's customers' personal information, the external party shall undergo an audit by internal or independent auditors, who will create an audit report at least once a year.

3.2 System Management

3.2.1 Inventory and Ownership

Create a system inventory that contains the classification details and ownership. Review the system inventory account at least once a year or when changes are made to the account.

3.2.2 Software Licensing Management

1) Use licensed software and only for operations related to the company.
2) Using hacking tools or other monitoring and securing information and systems software, such as software for testing and detecting vulnerabilities and software for hacking systems without permission, is prohibited.

3.3 Data Security Management

3.3.1 Security Classification and Handling

1) Data must be classified and handling appropriately in accordance with the company's *Data Classification and Handling Standard* document to ensure data security.
2) Data must be controlled throughout its lifecycle, including creation, usage, transmission, storage, and destruction, in a manner commensurate with the confidentiality and sensitivity of the data.
3) Electronic Data Handling
    a. Send the delivery of confidential company information via email or designated channels only. For details on the highly confidential level, attached documents must include password protection before sending, and the password must be sent separately via another channel, such as sending the document information via email and sending the password via SMS.
    b. Photography of the company data is prohibited—especially Customer personal information.
    c. Posting the company information on social media is prohibited.
    d. Request the company's permission before deleting and destroying essential company data; written approval must be granted.
4) Publishing Data Handling
    a. Printing confidential information, critical company information, and customer personal information in publishing media without the company's permission is prohibited.
    b. Approval must be granted before the deletion of confidential information critical company information. The document must be destroyed immediately according to international standards by cross-shred or strip-shred or shredding repeatedly until it cannot be reassembled into the original data.
5) A Data Processing Agreement (DPA) must be created and implemented if the third party has access to personal information.

3.3.2 Data Encryption

The company mandates that sensitive data, particularly personal information, must be encrypted both Data at Rest and Data in Transit, in accordance with company standards.

3.3.2.1 Data at Rest Data must be encrypted using the following encryption standards:

- Symmetric
    - ○ AES-128 or greater
- Asymmetric
    - ○ RSA-1024 or greater, particularly system components that are in-scope PCI DSS, Digital ID must be encrypted in RSA-1024 or greater.

- ○ ECC-224 or greater
- ○ DSA-2048 or greater
- ○ D-H-224 or greater

In case of using the sensitive data as the following must be encrypted by Field-Level encryption:

1) ID card or passport number, which included Laser ID, Chip ID, bp1no.
2) MSISDN (such as mobile number and IoT number), or FBB-ID
3) Account number
4) Credit card or debit card number

3.3.2.2 Data in Transit Data transmission must be encrypted using the following standard:

1) Using VPN connection: TLS version verification The VPN concentrator shall be configured to use TLS 1.2 (or greater). Prohibits the use of SSL 3.0 and below connections.
2) Using HTTPS connection: TLS 1.2 (or greater) and prohibits the use of SSL 3.0 and below connections.
3) Using other secure connection: Another connection is allow by using secured protocol such as FTP with secure encryption (SFTP), SSH (Shall not allow root login)

3.3.3 Data Asset Inventory Management

1) Third party must create a data asset inventory that specifies the names of data owners and controllers, purposes of storage, storage location, format/type of data storage, and duration of lawful basis of processing data storage. This process facilitates systematic and standardized data management and complies with the data handling guidelines.
2) Third party must review the data asset inventory at least once a year or when the system's asset inventory changes.

3.3.4 Data Retention and Archiving

1) Retain important information for a specified period. After the period specified in the Retention Period has elapsed according to the following table, ensure safe data deletion and destruction according to international standards to meet the purpose of data retention and comply with the company's *Data Retention Standard* document.

No.	Category	Retention Period	Lawful Basis / Data Management
1	6 Domains of sensitive data, including customer personal information	Retain throughout the service period according to the contract.	Service contract basis

No.	Category	Retention Period	Lawful Basis / Data Management
2	Log files	90 days from the date that data enters the computer system.	Section 26 Computer Crime Act

2) After the service contract has been canceled or ended, the third parties must transfer company data as well as essential data on projects jointly created for the company and delete and destroy data stored with third parties after the delivery of data is completed no more than seven business days, except in cases where it is necessary to retain personal information for compliance with applicable laws only.
3) Notify the deletion of the company's customers' confidential information and personal information to the project manager and get approval from the company first. In addition, always provide a data deletion report along with the evidence of data deletion for the company.

3.4 Human Resource Management

Third party involved in company projects must be provided with appropriate training on cybersecurity and personal data protection. This includes an assessment of their cybersecurity knowledge and understanding.

3.5 Subcontractor Management

In case there are subcontractors, the employee shall comply with the following:

1) <u>Subcontractors must sign a non-disclosure agreement as an individual or legal entity and agree to comply with this standard.</u>
2) The third parties must take the subcontractor's standard compliance and cyber risks and data protection assessment at least once a year.
3) Software development from subcontractors must be supervised, inspected, and operated using approved security standards. All third parties who develop software on behalf of the company must comply with the approved and signed contract, which must include the Property Rights, License Arrangement, Security Measures, Auditing Rights, and Testing Rights.

3.6 Physical and Equipment Security

3.6.1 Physical Access Control

1) Third party must have access control measures in place, dividing the area into zones based on risk levels and implementing appropriate access rights.
2) Must not disclose the location of essential company locations, such as data processing locations, executive room, and so others.

3.6.2 Access to Computer Systems

Restrict the computer system access to only those with related duties and permission granted.

3.6.3 Protecting Against Physical and Environmental Threats

The system used to process the company's essential data must operate as follows:

1) Computer system installation and storage location must have a safe environment from things that may harm the system. It should be suitable for work and convenient in solving computer system problems, such as having clear signs and alarm systems, an automatic fire extinguishing system, maintaining the temperature and humidity at appropriate levels, and having an electrical system ready to use in both standard and abnormal conditions.
2) Locations containing the company's critical information or systems must install a surveillance system to monitor for 24 hrs. daily (24x7).

3.6.4 Safe Destruction or Recycling of the equipment

Arrange the destruction of portable storage media per the data confidentiality levels to ensure that critical information and software are securely erased or overwritten according to international standards.

3.7 Communications and Operation Management

3.7.1 Operational Procedures and Responsibilities

3.7.1.1 Operating Procedures Document

Create and review the operating procedures document. The document shall contain data processing and management procedures, recommendations for handling errors, and details of departments supporting operations or other unexpected problems.

3.7.1.2 Change Management

1) Create the change management process and appropriate control over software, hardware, and communication network changes. Especially the production operating system, with at least the following topics covered:
   - Change Risk Assessment
   - Vulnerability Assessment

- Penetration Testing in case the system is a web application, application program Interface.
- Prepare rollback procedures in case of errors.

2) Any changes made to the computer system must be documented.

3) In cases where the company is the system administrator, the service providers must follow the company's change management process.

3.7.1.3 Separation of Development, Test, and Production Systems

1) The development, test, and production systems must be separated to handle critical data. The system separation requires physical access control and/or logical access control.

2) The company prohibits using production system data, essential data, personal information, or confidential information for system testing.

3.7.2 Capacity Management

1) Create a capacity planning process to determine the maximum capacity of resources in the computer system. Conduct regular monitoring and tuning of the efficiency of computer system resource usage to support the forecasted workload precisely.

2) Document the capacity management procedures. The procedures shall be promulgated and updated regularly.

3.7.3 Protection Against Malicious Software

1) Establish appropriate measures to prevent, detect, and/or modify all computer systems appropriately and protect against viruses and malicious software.

2) Install anti-virus, malicious software, and Endpoint Detection and Response, which the company authorizes. Those must be enabled and updated at all times, and running scans to detect malicious software.

3.7.4 Backup and Restoration

1) Regular data backups must be performed, and the security measures for storing backup data should be equivalent to those for storing the original data. This may include disconnecting backup systems from the network to protect against ransomware attacks.

2) Critical data recovery testing should be conducted at least once a year, and the test results should be documented in writing. This is to ensure that the recovered data meets the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified in the service level agreement (SLA).

3.7.5 Network Security Management

1) Create a detailed diagram showing the connections of various systems and devices. Consider this document as essential and reserve it for only responsible officers.

2) Establish network security management measures. Disable or disconnect ports when not using the device, protect the system and related applications, and have security status alerts when the network device fails.
3) Create measures to control monitoring tools, software, or programs that may cause security violations.

3.7.6 Removable Media Handling

1) Store removable media containing company's sensitive data in a secure location. And prevent unauthorized disclosure, whether intentional or unintentional.
2) Management of removable media containing company's sensitive data must be done by authorized persons only.
3) Deleting company's sensitive data on removable media must granted writing approval from the company each time beforehand. However, the destruction of sensitive data must be recorded as evidence for investigations.

3.7.7 Cloud Storage Management

1) The data stored on cloud storage must be limited to what is necessary and compliant with applicable laws and regulations.
2) Create regulations to control access to data and keep access logs in the cloud storage specified by the company.

3.7.8 Information Transfer

3.7.8.1 Information Transfer Policies and Agreements

Information transfer agreement between company must be established, and data must be controlled according to appropriate confidential levels.

3.7.8.2 Physical Removable Media in Transit

Limit the access to removable media containing company information or prohibit media use on devices or computers without permission.

3.7.8.3 Transmission Control Protocol

1) Encrypt data according to the standards set by the company when transmitting important information through the network, especially data that communicate with external networks.
2) Change the password used to protect the encryption key as soon as received and change to the new one at appropriate intervals regularly.
3) Specify the criteria for confirming accuracy with the original data for information related to financial approval.

3.7.8.4 Data Verification

Computer systems that transmit data must have their data transmission and reception verified using various methods, such as sequence number checking or data quantity checking. This is to ensure that the transmitted data is complete and correctly sequenced.

3.7.9 Monitoring

3.7.9.1 Log Data Management

1) Retain the activity log of system administrators and system operators. Check the recorded log regularly. Only authorized persons can access such logs.
2) Retain the audit log that stores user activities, usage exceptions, and essential systems' information security incidents within the period specified by law or operational requirements.
3) Prevent log facilities and log files from tampering and unauthorized access.
4) Store necessary devices or systems in a safe location.

3.7.9.2 Monitoring System Use

1) Retain logs, analyze errors in critical systems, and take appropriate action to reduce the chance of reoccurrence.
2) Regularly audit and review services and logs obtained from third party systems.

3.7.9.3 Computer Systems and Networks Time Synchronization

System clocks of computers and networks must be synchronized with a standard time reference. This synchronization should be performed using a reliable source, such as International Atomic Time (TAI) or Coordinated Universal Time (UTC). Additionally, procedures should be established to monitor and rectify any time discrepancies that may arise.

3.7.9.4 Intrusion Detection and Tracking

1) There should be criteria for reviewing the logs of computer systems to check for security breaches or attempts. This review considers relevant information and news about vulnerabilities and cyberattacks on computer systems and networks from various sources, such as websites with cybersecurity reports published by cybersecurity experts, product vendors, hacker groups, government organizations, or agencies related to cybersecurity. This is to ensure that any attempted or actual breaches are prevented and addressed promptly.
2) Retain the logs recording user activities, exceptions, and information security events shall be produced and kept at least 90 days.

3.7.10 Patch Management

1) Constantly update the patch to the current version. Monitor patch software to reduce attacks on possible vulnerabilities. The source of all patches must be reliable and accurate, and the patch must be correct and complete. All patches must undergo appropriate testing before being announced.

2) Update the firmware for servers, network devices, and appliance boxes related to security to the extent that they do not conflict with the system's operation. However, all new systems must use current patches. If there are exceptions, an action plan must be created and informed to the company's project managers, along with developing appropriate control measures to manage risks to an acceptable level.
3) The authorized third party devices necessary to connect with the company devices must be updated and configured before connection.
4) Back up data before updating any patches so that data can be recovered when a problem occurs.

3.8 Access Control Management

3.8.1 User Access Management

3.8.1.1 User Access Provisioning

1) The process of requesting access to information or computer systems:
   - In case of the third party owns the computer system, the third party must establish a process for user registration and request access to information or the computer system.
   - In case of the third party access the company's information or computer system, the third party shall comply the company's process for user registration and request access.
2) Specify the username (User-ID) of users and administrators using the principle "one person per username" only. Do not use the same user ID or use one user ID for many people.
3) Follow the user rights modification process when users change their roles and responsibilities.
4) A process must be established for revoking or suspending users' access to systems and services. This includes removing users from the user registry within 3 business days of the revocation or suspension taking effect.

3.8.1.2 Privilege Management

1) Requesting new rights and additional rights to access computer systems and services must be granted according to roles and responsibilities and as necessary to perform the job (Least Privilege)
2) Requesting a username (User-ID) with special privileges, such as administrator:
   - In case of the third party owns the computer system, third party must establish an expiration date for privileges and should designate a separate user account for system monitoring purposes that does not

require privileged access. Privileges should be limited to what is necessary for routine system monitoring only.

- In case of the third party access the company's information or computer system, authorization will be granted strictly on a need-to-access basis. The company reserves the right to set a maximum expiration period of one year per authorization. Individuals must undergo training in Centralized Remote System knowledge and pass an assessment with a score of at least 90% before being granted access privileges.

3) When accessing systems with sensitive information, use multi-factor authentication.

3.8.1.3 User Identification and Authentication

1) Uniquely identify and authenticate all computer system users and consistent with the system data's level of importance. The system must be able to log out automatically when the specified period has elapsed after the user's session ends.
2) Unauthorized access to authentication data storage is prevented, and logs of all processes carried out by users are recorded.

3.8.1.4 Setting the Automatic Logout Time

Set a time to automatically log the users out of the system at the specified time or when the user has not used the system within the specified time. A system that connects or provides the company's critical information and customers' personal information should last for no more than 10 minutes and no more than 15 minutes for any other system.

3.8.1.5 Review of User Access Rights

1) The user's access rights should be regularly reviewed by a third party, at least once a year, and the system must demonstrate overlap or conflict access rights. Users whose rights have been revoked or are inactive must be immediately removed from the system to prevent unauthorized access.
2) The responsible person must regularly audit and inspect at least once a year to ensure that no usernames (User-ID) have been left in the system for a long time. Provide the old username (User-ID) to the new user, or consider only necessary and sufficient for use. Modify user rights when the users change their job role or are granted the right to access personal information.
3) The responsible person must regularly review the user rights and immediately cancel the user's access rights when users change their job roles or resign.

3.8.2 Password Management

3.8.2.1 Use of Password

1) Change the password and any other codes when the old one expires or when it is considered appropriate to change.
2) Do not store passwords in clear text.
3) Display and password input must be masked or used in other secure ways to prevent unauthorized people from noticing the password.
4) Passwords must not be hard-coded in the computer system without a mitigation control.
5) Passwords must be sent in an encrypted format to prevent attacks from malicious actors.
6) Do not use the password set by the system (Default). The system must require the user to change the password immediately after logging in for the first time or when installing a new system or updating computer systems.

3.8.2.2 Password and Username (User-ID) Security

1) Passwords and any other codes designated by the company as confidential details must be kept so that others do not know or share them with others.
2) Determine the passwords' minimum length and lifetime following the requirements classified by the type of user group as follows:
   - The user level requires a password that is at least 12 characters long and changes the password at least every 90 days.
   - The privileged users set a password that is at least 20 characters long and change the password at least every 90 days.
   - The service accounts set a password that is 30 characters long and change the password at least every year.
3) Passwords ought to possess the following qualities:
   - A combination of capital letter, non-capital letter, number, and special character such as @ or #.
   - Not a running number e.g. 12345678.
   - Not a predictable word or a plain word from a dictionary such as “password”.
   - Password history is set at least 5 times. User shall be prevented from using the same previously used passwords.
4) Sensitive systems shall accept no more than five password entry errors or comply with related legal requirements, regulations, and the company announcement. If the next password entry is incorrect and exceeds the specified number of times, the computer system must temporarily suspend the user's session immediately.

5) Sensitive systems must be able to check past user passwords to prevent reusing the old password. The system must be able to check back at least five times or as required by related laws, regulations, and the company announcement.

6) Create measures to prevent quickly random or guessed passwords, such as using passwords with one's name spelling, using the same password as the username, or leaving it blank.

7) Establish a safe method to distribute passwords or usernames (User-ID) to users.

3.8.3 Clear Desk and Clear Screen Policy

1) Log out or log off every system when not used for a long time. And turn off your computer and other connected devices immediately after work.

2) Control assets such as paper, removable storage media, and control system operating screens (Clear Screen Practice) to manage risks to important information.

3) Determine the procedures for destroying removable storage media and destruction of electronic data and files in electronic media that are standard and cannot be recovered and reused.

3.8.4 Access Control

3.8.4.1 Network Access Control

1) Implement network segregation as well as appropriate security control measures. Determine network usage where users can access only the authorized information system.

2) Restrict network access from a third party to company networks to authorized persons only. And require a secure authentication to prevent fake identification.

3) Establish a unique password or access control mechanism consistent with the company's standards to control access to all internal network devices, including routers, firewalls, and servers.

4) The responsible department must authorize devices connected to the network and the connection must be evaluated for impact and network compatibility.

5) The third parties accessing network devices must undergo a strong multi-factor authentication.

3.8.4.2 Remote Access

1) The company's remote access must include strong multi-factor authentication and all access logs.

2) Limit access from the third party to required systems, devices, and protocols to support work in line with the contract. In cases where remote access is permitted to the third party, the system must be enabled only for the specified period.

3) Those responsible for developing the system can access the production system only as necessary and occasionally. However, permission to use the system must be suspended as soon as it is no longer required.

3.8.4.3 Operating System Access Control

1) Determining rights for those who can use commands, set up, change program data, tools, or do any other actions that may be at risk for using the computer system, programs, or data. Consider the permission only based on absolute necessity and consistent with the duties assigned.
2) Set up the session time-out when there is a period of absence from use to prevent access from unauthorized third parties.
3) Limit the system connection time (Restriction on Connection Time) for more security for critical systems or applications.

3.8.4.4 Application and Information Access Control

1) Strictly control access to important company information, including all program source code, and must not inappropriately disclose, alter, or delete the data.
2) Limit the activities or personal information of each user according to their rights.
3) Implement appropriate physical and environmental controls for critical systems.

3.8.5 Mobile Computing and Teleworking

3.8.5.1 Personal Computer and Mobile Devices

1) Personal computers and mobile devices used for work-related purposes and devices allowed to connect directly or through other devices to the company's network, the following requirements must be met:
   - The devices must use licensed and up-to-date software.
   - The devices must be protected by antivirus software authorized by the company.
2) Every user must be aware of the safe storage of the company's data on mobile devices at all times.
3) Separate the susceptible system that is highly important to the organization from other systems, have a precisely controlled environment, and control personal computers, mobile devices, and teleworking.

3.8.5.2 Teleworking

The telecommuters must follow the policy and related security procedures and comply with the software license agreement and data backup.

3.9 System Acquisition, Development and Maintenance

3.9.1 Security Requirements for Systems

1) Develop the computer systems or applications with cyber security in mind from the design and setup stages according to the principles of security by design and security by default.
2) All project managers must ensure that security requirements, including security analysis, risk assessment, and vulnerability assessment, are collected and used as essential for procuring, developing, or improving new computer systems. Apply the security requirement throughout every step of the computer system development cycle.
3) The third parties involved in software development must be bound by approved and signed contracts. All third party software development must comply with the company's software development standards and security requirements equivalent to company requirements.

3.9.2 Correct Processing in Applications

1) Specify the requirements for ensuring the authenticity and integrity of data in the application. Control the criteria and implement them appropriately.
2) Imported and exported data from the application must be verified to ensure that it is accurate and appropriate and must be subject to operations or activities specified by the company only.

3.9.3 Cryptographic Controls

1) Implement the cryptographic key management to comply with encryption techniques, refer to subject *3.3.2 Data Encryption*.
2) Implement cryptographic control in a computer system classified as having the highest level of confidentiality, refer to subject *3.3.2 Data Encryption.*
3) Strictly restrict access to the encryption key. The person responsible for managing essential keys must go through a background check process and operational security audit, and have signed a non-disclosure agreement only.

3.9.4 Security of System Files

1) The company strictly prohibits the installation of inappropriate or unauthorized software on computer systems.
2) Implement security controls for system files such as, data encryption and access control, to prevent and mitigate the leakage of sensitive information.
3) Software and program library installation or update must be conducted by authorized personnel and proceed under the change management.

3.9.5 Security in Development and Support Processes

3.9.5.1 Technical Review of Application After Operating System Changes

1) Adequately test the major operating system and application changes to ensure that there is no impact on the security or operations of the company.

2) The third party shall communicate all system changes to Company's Project Manager.

3.9.5.2 Restriction on Change to Software Package

Risks associated with software package changes are appropriately controlled and approved.

3.9.6 Vulnerability Management & Penetration Testing

1) Set up system hardening to reduce cyber security risks, including critical systems.
2) Conduct an assessment to find vulnerabilities in computer systems connected to the network. If vulnerabilities are found, an assessment must be conducted and controlled by appropriate measures to reduce the risks to an acceptable level.
3) Inform the company's project manager about the implementation plan, including the tools used in the operation, and request written permission from the company every time before conducting the vulnerability assessment and penetration testing.
4) The company reserves the right to conduct vulnerability assessments and penetration tests, including other activities related to security simulations such as Red Team Exercises and Attack Surface monitoring, on systems that provide customer services without prior notice.
5) Regularly conduct a vulnerability assessment and penetration testing following the requirements or when there are any major changes to all internet-connected systems to identify security vulnerabilities and assess overall security. The company has determined the frequency of vulnerability assessment and penetration testing as follows:

System Type	Vulnerability Assessment	Penetration Testing
High-Priority/Significant System	1 time/year	1 time/year
Medium-Priority System	1 time/ 24 months	1 time/ 24 months
Low-Priority System	1 time/ 36 months	1 time/ 36 months
System related to PCI DSS	4 times/year (Quarterly)	1 time/year
System related to CSA Star	1 time/year	1 time/year
System related to ISO	1 time/year	1 time/year
System regulated by the Bank of Thailand (BOT)	1 time/year	1 time/year
Systems related to NDID and Public IDP	1 time/year	1 time/year

6) If vulnerabilities are found through vulnerability assessment and penetration testing, proceed to resolve under to the company's standards as follows:

- In case of a new computer system/application/feature, it shall be able to go into production by following these steps:

Critical / High severity	Medium Severity	Low Severity
Must resolve first.	1. Send a plan to fix vulnerabilities to the company's project manager within 15 days of receiving the latest assessment results. 2. Fix vulnerabilities within 60 days of receiving the latest assessment results. In case when it reaches the planned time but is still unable to fix the vulnerabilities, one must notify the company's project manager to enter the risk acceptance form	1. Send a plan to fix vulnerabilities to the company's project manager within 15 days of receiving the latest assessment results. 2. Fix vulnerabilities within 90 days of receiving the latest assessment results. In case when it reaches the planned time but is still unable to fix the vulnerabilities, one must notify the company's project manager to enter the risk acceptance form

- If vulnerabilities are found through vulnerability assessment and penetration testing under the company's schedule, proceed as follows:

Critical / High severity	Medium Severity	Low Severity
1. Send a plan to fix vulnerabilities to the company's project manager within 15 days of receiving the latest assessment results. 2. Fix vulnerabilities within 45 days of receiving the latest assessment results. In case when it reaches the planned time but is still unable to fix the vulnerabilities, one must notify the company's project manager to enter the risk acceptance form	1. Send a plan to fix vulnerabilities to the company's project manager within 15 days of receiving the latest assessment results. 2. Fix vulnerabilities within 60 days of receiving the latest assessment results. In case when it reaches the planned time but is still unable to fix the vulnerabilities, one must notify the company's project manager to enter the risk acceptance form	1.Send a plan to fix vulnerabilities to the company's project manager within 15 days of receiving the latest assessment results. 2.Fix vulnerabilities within 90 days of receiving the latest assessment results. In case when it reaches the planned time but is still unable to fix the vulnerabilities, one must notify the company's project manager to enter the risk acceptance form

3.10 Cyber Security Incident Management

1) Establish a cyber security incident management process to handle cyber security incidents and prepare documents for operational procedures, which covers the importance and structure for reporting cyber security incidents to relevant departments and communicating with employees and appropriate third parties.
2) Create a cyber security incident response plan following the risks involved and use it to communicate and train appropriately to those involved.
3) Prepare some secure tools and techniques for investigating events on computer systems, attack detection, and displaying unauthorized use of computer systems.
4) Review the cyber security response plans at least once a year, starting when the plan is approved.
5) Designate at least one person as the person responsible for cybersecurity. This person will be responsible for:
    - Coordinating and notifying the company in the event of a cybersecurity incident.
    - Coordinating with the company's employees if the company discovers a cybersecurity incident involving an external party.
6) In the event of a cyber security breach that has an impact on the company, the third parties must report the incident together with the available details of the incident to the company without delay

within 12 hours, and when there is progress or additional information, notify the company periodically and quickly prepare the details of the notification letter to the company.

3.11 Business Continuity Management

1) Create a business continuity plan and disaster recovery plan that cover service providing, connections, or information accessing from third parties to have guidelines to support and provide services and conduct business continuously.
2) The business continuity plan and disaster recovery plan should consider risks that may result in service disruptions, connectivity, or access to information from third parties, impact on service and communication between the third party and the company, and promptly report unusual events to the company.
3) Test and modify the business continuity and disaster recovery plans that cover service providing, connections, or data accessing from third parties at least once a year.
4) Third party shall encourage or take part in the company's Business Continuity Plan Testing activities.

3.12 Regulatory and Compliance

1) The third parties must comply with legal requirements, rules and regulations related to company service providing in cyber security, personal information protection, requirements of the company's regulator, other laws, and related contracts.
2) The third parties must keep business information as required by laws, regulations, and related contracts for business purposes before destroying the data.
3) Third parties must maintain information confidentiality according to the non-disclosure agreement for business purposes and not disclose confidential information to others and the public.

Effective date: From 15 July 2024 onwards.