Unofficial Translation

This translation is for convenience of those unfamiliar with Thai language.

Please refer to the Thai official version.

Bank of Thailand Notification

No. SorNorChor. 11/2561

Re: Policies and Measures on Security of Information Technology Systems

---

1. Rationale

To provide standards in prescribing of policies and measures on security of information technology systems for service providing of the Highly Important Payment Systems, the Designated Payment Systems and the Designated Payment Services according to the law governing payment systems; and to use as the guidelines on determination of procedures of audit and security measures of information technology systems relating to the highly important payment systems, the designated payment systems and the designated payment services. This is to ensure that such information technology systems shall be reliable, secure and capable of operating continuously.

The Bank of Thailand (BOT) has defined the framework for policies and measures on security of information technology systems which consist of 1) Access control and authentication 2) Information confidentiality and system integrity 3) Service availability and 4) Security audit of information technology systems. This aims to use them as the guidelines on determination of security measures of information technology systems relating to the highly important payment systems, the designated payment systems and the designated payment services; and in order to ensure the security measures should cover and prevent from the risk of information technology systems efficiently in compliance with the international standard guidelines. Besides, the service providers of the highly important payment systems and the business providers of the designated payment systems and the designated payment services shall apply and design on security measures of information technology systems in associated with types and complexity of their own services.

2. Statutory Power

By virtue of Section 7 and Section 24 of the Payment System Act B.E. 2560 (2017), the Bank of Thailand hereby prescribed the guidelines on Policies and Measures on Security of Information Technology Systems for the service providers of the highly important payment systems, the business providers of the designated payment systems, and the designated payment services, as prescribed in this notification.

3. Scope of Application

This Notification shall be applied to the service providers of the highly important payment systems, the business providers of the designated payment systems and the designated payment services in accordance with the law governing payment systems.

4. Content

4.1 Definition

In this Notification,

"Service Provider" means the service provider of the highly important payment system under the law governing payment system.

"Business Provider" means the business provider of the designated payment system and the business provider of the designated payment service, under the law governing payment system.

"Member" means a system user who agrees to be bound by the rules of a highly important payment system.

"Service user" means the user of services provided by the business provider with license or registration under the law governing payment system.

4.2 Security policies and measures of information technology systems

The service providers of the highly important payments system, the business providers of the designated payment systems and the business providers of designated payment services shall comply with the policies and security measures of information technology systems as follows:

4.2.1 Security Policies of IT Systems

(1) The service providers or the business providers shall establish the written security policies of information technology systems with an approval from the Board of directors (Board). In this regard, the service providers or the business providers shall circulate such policies and organize the training for related staff to ensure the compliance with the policies, including the review or adjustment as deemed appropriate to the current situations on a regular basis.

(2) The security policies of information technology systems relating to the highly important payment systems, the service providing of the designated payment systems and the designated payment services, as the case may be, must at least include the following areas:

(2.1) Access control and authentication

(2.2) Information confidentiality and system integrity of information technology systems

(2.3) Service availability

(2.4) Security audit of information technology systems

4.2.2 Security Measures of Information Technology Systems

The service providers or the business providers shall establish the security measures of information technology systems relating to the highly important payments system, or the designated payment systems or the designated payment services, as the case may be, in accordance with the prescribed policies. Such measures must be appropriate for the characteristics of the service which include the access control and authentication, information confidentiality, integrity of the information technology systems, service availability, incident response and report including regular security audit at least on an annual basis. As well, the monitoring process should be set up by the Board or the senior management to ensure the compliance with the prescribed measures. In this regard, the security audit of information technology systems of the service providers of the highly important payment systems, the business providers of the designated payment systems and the designated payment services, shall also be in compliance with the notification of the BOT relating to the supervision guidelines.

Besides, the service providers or the business providers must review and revise measures according to the specified period, or when there is any change causing an

impact on the policies and measures, as well as provide the training and education to the related personnel.

In this regard, the BOT has prepared the guidelines on security of information technology systems to be used for establishing the security measures of information technology systems to be credible and accepted by the service users. Furthermore, determination of the security measures of each service provider or business provider may vary in order to cover and prevent from the risks of information technology systems efficiently in compliance with the international standard guidelines.

5. Transitional provision

For those who provide the service on the highly important payment systems or those who undertake the designated payment system or the designated payment service prior to the effective date of this notification, if they cannot propose the security policies of information technology systems to the Board for approval, as prescribed in Clause 4.2.1 (1), they shall be exempt from the regulation. However, they shall manage to comply with such regulation within 90 days from the day that permission or registration has been granted, as the case may be.

6. Effective Date

This Notification shall come into effect from the 16 April 2018 on wards.

Announced on 16th April 2018

(Mrs. Ruchukorn Siriyodhin)
Deputy Governor, Financial Institutions Stability
Governor for
Bank of Thailand

Payment Systems Policy Department
Tel. 0 2283 5036, 0 2283-6718

Guidelines on Security of IT Systems relating to the Payment Systems

To promote the service providing of the highly important payment systems, the undertaking of designated payment systems and the designated payment services to be efficient, secure, accurate and reliable, the Bank of Thailand has established the guidelines or general framework on security measures of information technology systems. The service providers or the business providers may also establish the security measures to be appropriate for types and complexity of their own services.

Essential contents of these guidelines consist of:

1. Access Control and Authentication

The service providers or the business providers shall consider about assignment of staff or units to be responsible for the information technology and the appropriate separation of duties, access control to information technology systems, authentication and the prevention of denial of liability, as follows:

1.1 Assignment of staff or units to be responsible for the information technology and the separation of duties appropriate for the management of information technology systems.

The service providers or the business providers shall assign duties and responsibilities to staff or units accountable for security of information technology systems as well as create awareness, provide knowledge and train the staff in the organization including create the disciplinary procedures for punishment in case where there is violation or breach of security rules & regulations.

Guidelines:

(1) Define duties & responsibilities and clearly separate duties in each area of security of information technology systems, ensure checks & balances, in order to prevent the operational risks that might happen.

(2) Provide training, education and create awareness including communicate to the personnel in the organization on a regular basis in order for staff to keep up with technology and various new threats.

(3) Establish disciplinary procedures to punish those who violate or break the policies or regulations relating to security of information technology systems.

1.2 Access Control to Information Technology Systems

The service providers or the business providers shall establish written procedures for controlling and limiting the access rights to the information technology systems relating to service and information as needed, in order to prevent the hacking or access into the system of the unauthorized people from both inside and outside the organization.

Guidelines:

(1) Set up a registration of assets or information technology equipment to be accurate as well as assign the person in charge.

(2) Establish appropriate rules and regulations for the use of information technology systems and the related assets or equipment.

(3) Provide control and preventive measures of access to location, equipment and information technology systems relating to the service. Such processes should include:

(3.1) Place or install the equipment for service in the separate area, provide the restricted area for important equipment together with control over it in order to prevent the unauthorized access to the facilities from both inside and outside the organization.

(3.2) Establish and manage procedures and access rights to the information technology systems relating to service in accordance with authority level, as well as verify the access rights of members, service users, and related personnel before granting the access permission to the systems. The process should be reviewed and updated on a regular basis.

(3.3) Record each access log to information technology systems of members, service users and related personnel for the use of tracking and auditing the abnormalities that might happen, as well as ensuring the regular review by the responsible units for security measures or by the independent units.

1.3 Identity Verification and Prevention of Denial of Liability

The service providers or the business providers shall provide identification, authentication or verification of user identity by using appropriate technology to be associated with the risk level of each business type e.g. the use of password, personal identification number, token or smart card, biometric characteristics or public key infrastructure in order to prevent denial of liability in case of dispute.

Guidelines:

(1) Having procedures for identification or authentication or verification of identity before accessing the information technology systems of members, service users and related personnel in order to ensure the access by the authorized person is valid. This includes prevention from denial of liability or dispute in making transaction.

(2) Record details of access to information technology systems and keep it as the evidence for examination in case of any problem and to prevent from denial of liability.

2. Information Confidentiality and System Integrity

The service providers or the business providers shall establish the measures on information confidentiality and service system integrity such as developing, controlling, adjusting, improving the system or equipment used for information processing, and managing the network systems relating to service in order to ensure the system integrity

2.1 Information Confidentiality

The service providers or the business providers shall establish the appropriate steps and procedures in transmitting, processing and storing information in order to preserve confidentiality and accuracy of information.

Guidelines:

(1) Determine the level of information confidentiality according to the level of its importance and determine the access rights to such information. This should include management and preservation of data privacy of the members or service users to be in compliance with the related regulation or law.

(2) Establish procedures in transmitting, processing and storing confidential information strongly and securely according to the level of importance in order to prevent the adjustment of information from the unauthorized persons.

(3) Establish procedures in storing, using and destroying of information with each confidential level.

2.2 Development of systems, Change control management, Improvement of information technology systems or data processing equipment.

The service providers or the business providers shall establish systematic procedures and internal control for developing and controlling over changes or improvement of information technology systems to reduce the risks of failure or malfunction of service systems.

Guidelines:

(1) Having process of system development to be accurate and reliable which covers the process of system designing, developing, testing and implementing, together with the vulnerability assessment and penetration test performed by the external expert for the significant systems that connect with the public networks prior to implementation. Additionally, it should separate the system for development from the system for production; it can be the separation of equipment with different controllers.

(2) Having procedures to control the revision or alteration of information in the process of data processing, data transmitting, storing, acquiring, improving of equipment and developing of information technology systems. For example, there should be procedures for related impact assessment, approval from authorized person, development or improvement, pre-production test, as well as the procedures for recording any revision or change, notifying those who are affected from such changes and updating the related documents.

(3) Outsourcing of information technology activities

(3.1) Develop the service contracts in writing with clear scopes of operation, duties and responsibilities of each parties.

(3.2) Establish the appropriate risk management for the outsourcing activities including selection, monitor, evaluation and examination of service provided.

(3.3) Establish preservation of information security which includes confidentiality and data privacy of the members or service users.

(3.4) Resume responsibility to members or service users for service continuity, security and credibility as if the services are provided by the service providers or the business providers themselves.

(3.5) Prepare the emergency plan for information technology operation of the service providers of outsourcing activities to be consistent with the emergency plan of the service providers or the business providers.

(4) Prepare manuals relating to the information technology systems used in service, as well as train and distribute to all staff for implementation.

2.3 Management of network systems relating to service

The service providers or the business providers shall establish the preventive measures for the unauthorized access to the network system of services.

Guidelines:

(1) Manage service networks in order to prevent cyber threats or the information transmitted through the network such as:

(1.1) Establish the measures for controlling the network connection, and for granting permission to connect with the external equipment.

(1.2) Authentication for accessing the network

(1.3) Separate networks associated to group of information technology service

(1.4) Install software or firewall to prevent the external threats.

(2) Have the efficient measures to control and prevent other threats and have it updated on a regular basis.

3. System Availability

The service providers or the business providers shall provide services with efficiency and high availability to adequately support each transaction of members or service users as needed and rapidly respond to transaction making in both normal and peak time including an appropriate information back-up to ensure system recovery in case of system damage.

3.1 Risk assessment and management of service system

The service providers or the business providers shall ensure the appropriate risk assessment methodology of service system, determine criteria for risk appetite and risk tolerance and procedures to manage the potential risks. In this regard, the service providers or the business providers shall regularly conduct the risk review in associated with technology development and current situations.

Guidelines:

(1) Establish the concrete methodology for risk assessment.

(2) Analyze and evaluate the impacts on business that may result from the failure of security measures.

(3) Determine criteria for risk appetite and risk tolerance

(4) Identify and evaluate alternatives in managing operational risk that may occur in order to avoid risk and mitigate potential damages.

3.2 Monitor and detect abnormalities or vulnerabilities of the information technology systems

The service providers or the business providers shall monitor and detect abnormalities and also follow the news about vulnerability of various systems used in service in order to evaluate risks and determine measures for risk mitigation.

Guidelines:

(1) Monitor and detect the unusual transactions and the opportunity of threats or the unauthorized access to information technology systems.

(2) Assess vulnerability of the system and prepare the measures to resolve or close system vulnerability, especially in the network service systems as well as the application software and database.

(3) In case of the system with high risk such as the service system connected via the public networks, the penetration test should be conducted to test the efficiency of security technology.

3.3 Resolution, Incident response, recording and reporting in case where the damages occur to the information technology system.

The service providers or the business providers shall monitor, record, and report the incidents of security breach via the defined reporting channels as soon as possible. Moreover, the lesson learnt from the past experiences shall be taken into account for the advance preparation of necessary preventive measures.

Guidelines:

(1) Establish procedures for problem solving with responsible team or staff, reporting line to management and notifying related parties.

(2) Gather useful and related evidences.

(3) Record incidents or write up the report in order to keep it as guidelines for problem solving.

3.4 Information backup

The service providers or the business providers must have information backup and it must be regularly validated in order to preserve its accuracy, completion and availability of the service.

Guidelines:

(1) Create the backup of important information and other necessary information for operation in order to ensure information availability within the country for business operation and service providing to the customers with continuity.

(2) Establish appropriate guidelines or procedures for information backup in associated with related risks or service characteristics of the highly important payment systems, or the service of the designated payment systems and the designated payment services, as the case may be, such as information for backup, frequency, media to be used, storing places, preservation methods and information restoration.

(3) Regularly validate the information backup at least on an annual basis in accordance with the information backup policies of the service providers or the business providers.

3.5 Development of business continuity plan or emergency plan of IT systems.

The service providers or the business providers shall develop the business continuity plan for service of the highly important payment systems, the designated payment systems or the designated payment services, as the case may be, and implement the plan to ensure the service can proceed within the defined timeline after the incident of service suspension occurred.

Guidelines:

(1) Analyze and identify the important risks and operation of service.

(2) Determine recovery time objectives

(3) Establish the plan in writing with procedures and details of operation when a suspension of important operation occurs in order to be able to recover the operation within defined timeline. The details of plan shall at least consist of the followings:

(3.1) Name of plan

(3.2) Objectives and scopes of plan

(3.3) Details of IT system, necessary resources for replacement of operation

(3.4) Responsible persons, authorized person, communications or call tree with the related persons from both outside and inside the organization.

(3.5) Implementation practices or manual in case where the problems occur, and reserved location for replacement of operation.

(4) Regularly conduct the training to staffs and related parties of the plan.

(5) Test and review the plan for the important operations at least on an annual basis or when there are any changes of factors affecting the risk.

3.6 Maintenance of the equipment of information technology system

The service providers or the business providers shall provide the regular maintenance of equipment in order to ensure its continuity and good condition for usage.

4. Security Audit of Information Technology Systems

The service providers or the business providers shall provide a security audit of information technology systems at least on an annual basis in order to ensure the policies and measures on security of information technology systems are efficient and secure so that the services can be provided with continuity. They must submit a copy of an audit result to the BOT within 45 days from the audit completion date.

Guidelines:

(1) Provide an auditor to perform security audit of information technology systems in the areas prone to risk or essential to the service at least on an annual basis. Prepare an audit report to the Board of directors or the assigned Board of directors for consideration of existing risks and determination of guidelines on improvement, as well as notify the related internal units for implementation.

(2) Monitor, examine the service of the highly important payment system, the designated payment systems and the designated payment services, as the case may be, to be in compliance with all related rules and regulations in order to avoid violation of legal requirements, regulations, agreements on contract as well as the security requirements.

5. Review or Improvement on Security Measures of Information Technology Systems

The service providers or the business providers shall review or revise the security measures on information technology systems at least on an annual basis or when there is any change causing an impact on policies and measures, as well as provide the training and education to the related personnel.

Besides, the service providers or the business providers should ensure readiness of security measures of information technology systems in order to cope with cyber threats. This should include the supervision of risks from cyber threats such as protection, detection, response and recovery which should be in accordance to its necessity, risks and complexity of the service.

Payment Systems Policy Department
The Bank of Thailand