Unofficial Translation

Volume 127 Part 53 Ngor Government Gazette 3 September 2010

Royal Decree

Regarding Security Techniques in Performing Electronic Transactions

B.E. 2553

BHUMIBOL ADULYADEJ, REX.

Given on the 23rd Day of August B.E. 2553;

Being the 65th Year of the Present Reign.

His Majesty King Bhumibol Adulyadej is graciously pleased to proclaim that:

Whereas it is expedient to prescribe the Security Techniques for Electronic Transactions.

By virtue of Section 187 of the Constitution of the Kingdom of Thailand and Section 25 of the Electronic Transactions Act B.E. 2544, which contain certain provisions relating to the restriction of personal rights and freedom, for which Section 29, incorporating Section 43, of the Constitution of the Kingdom of Thailand provides that it can be made by virtue of the provisions of a law. Therefore, His Majesty the King hereby enacts this Royal Decree, as follows:

Section 1 This Royal Decree is called the "Royal Decree on the Security Techniques in performing Electronic Transactions B.E. 2553".

Section 2 This Royal Decree shall come into force after one hundred and eighty days from the date of its publication in the Government Gazette.

Section 3 In this Royal Decree:

"Security Techniques" means the Security Techniques in performing electronic transactions.

"Informational Assets" means:

(1) computer network system, computer system, computer work system and information system;

(2) computer machines, computer equipment, information recorders and any other equipment; and

(3) information, data messages and computer data.

"Information Security" means the protection of illegal access, use, disclosure, obstruction, change, acts causing loss, damage, destruction or access to the knowledge of Informational Assets.

"Administrative Security" means an act at executive level in providing any policy, measure, rule or process for use in the process of selection, development, use or maintenance of Informational Assets in a secure manner.

"Physical Security" means an act of providing any policy, measure, rule or any process for use in preventing Informational Assets, or any other assets from threat by a person, natural disaster, accident or any other physical disaster.

"Confidentiality" means preventive maintenance or preservation of the computer network system, computer system, computer work system, as well as the information system, information, data messages or computer data from access, use or disclosure by any unauthorised person.

"Integrity" means an act of ensuring completeness of information, data messages or computer data during use, processing, transfer or archive, in order to prevent any unauthorised or illegal change, loss, damage or destruction.

"Availability" means an act of ensuring that the Informational Assets are functional, accessible or usable during any time required.

"Critical Infrastructure" means an agency or organisation, or any part of the agency or organisation, in which the electronic transactions of such agency or organisation, or any part of the agency or organisation, have material consequences to the security or public order of the country or the general public.

Section 4 There are three levels of Security Techniques, as follows:

(1) Strict level

(2) Medium level

(3) Basic level

Section 5 Security Techniques according to Section 4 are for use in the following electronic transactions:

(1) Electronic transactions which have an impact on the security or public order of the country or the general public.

(2) Electronic transactions of the agency or organisation, or any part of the agency or organisation, which are deemed to be Critical Infrastructure.

Section 6 The Commission shall issue notification(s) specifying the categories of electronic transactions, or the rules on impact level assessments of electronic transactions, pursuant to Section 5(1), which shall be in accordance with the Security Techniques in the strict level, medium level or basic level, as the case may be; provided that the level of the Information Security risk, the impact with regard to the value and damage which may happen to the service user, and the impact to the country's economy and society, must be taken into consideration.

The Commission shall issue notification(s) specifying the names or categories of the agencies or organisations, or any part of the agencies or organisations, which are deemed to be Critical Infrastructure pursuant to Section 5(2), which shall be in accordance with the Security Techniques in the strict level, medium level or basic level, as the case may be.

Section 7 The Security Techniques in each level, pursuant to Section 4, shall have an Information Security measure according to the rules that the Commission has notified. Such measure for Security Techniques in each level may have different rules as necessary, but shall have at least one of the following specifications relating to rules:

(1) Formation of Administrative Security.

(2) Creation of Information Security infrastructure with regard to the part of the Administrative Security of such information system, both internally and externally, for the agency or organisation.

(3) Management of Informational Assets.

(4) Formation of personnel Information Security.

(5) Formation of Physical and Environmental Security.

(6) Management of the communication and operation of the computer network system, computer system, computer work system and information system.

(7) Access control of the computer network system, computer system, computer work system, information system, information data, data messages and computer data.

(8) Procure or create development and maintenance of the computer network system, computer system, computer work system and information system.

(9) Management of unwanted or unexpected Information Security incidents.

(10) Management of the service or operation of the agency or organisation to ensure continuity.

(11) Audit and assessment of compliance with any policy, measure, rule or process, including the Information Security's requirement.

Section 8 For the benefit of having a guideline for making the Policy or Practice Statement regarding the Information Security of the agency or organisation, the Commission may specify or provide a technological standard which is generally accepted as a reliable technological standard in its notification, in accordance with Section 7.

Section 9 For any electronic transaction made through a procedure which has Information Security at a level equivalent to or not lower than the Information Security standard pursuant to the notification in accordance with Section 7, which has been prescribed as the level of Security Techniques in conducting such electronic transaction, such electronic transaction shall be presumed to have been made by a reliable method pursuant to Section 25 of the Electronic Transactions Act B.E. 2544.

Section 10 In performing an electronic transaction in accordance with the Security Techniques pursuant to this Royal Decree, such person shall consider the basic principles of Confidentiality, Integrity and Availability, and shall comply with the Policy and Practice Statement regarding the control of work and Information Security of such agency or organisation.

Section 11 In case the Commission perceives that any agency or organisation, or any part of the agency or organisation, has created its Policy and Practice Statement regarding the Information Security in accordance with the Security Techniques in performing electronic transactions pursuant to this Royal Decree, the Commission may notify and disseminate a list of names of such agency or organisation, or any part of the work of such agency or organisation, for general public knowledge.

Section 12 The Commission shall consider reviewing the rules regarding the Security Techniques in performing electronic transactions pursuant to this Royal Decree, including other related laws, at intervals of at least every two years, from the date on which this Royal Decree came into force. Consideration must be given to the appropriateness and alignment with technology which has been developed or changed, and report must be provided for submission to the cabinet.

Section 13 The Prime Minister shall have charge and control of the execution of this Royal Decree.

Countersigned
Abhisit Vejjajiva
Prime Minister

Remarks: The reason for issuing this Royal Decree is that, at present, information technology and communications have played an important role in the operation of both the public and private sectors. Electronic transactions are widely performed. Thus, it is appropriate to promote management of the security of Informational Assets in conducting electronic transactions. This is to ensure increased acceptability and confidence in data messages. Moreover, Section 25 of the Electronic Transactions Act B.E. 2544 prescribes that any electronic transaction made in accordance with the Security Techniques prescribed in the Royal Decree is presumed to be made by a reliable method. Therefore, enactment of this Royal Decree is necessary.