Volume 127 Special Part 78 Ngor Government Gazette 23 June 2010

Notification of the Electronic Transactions Commission

Subject: Policy and Practice in the Information Security of a State agency B.E. 2553

As both domestic and overseas Information Security issue is becoming more serious and tends to cause more impact on the public sector and business sector, this makes an operator as well as organisation, public sector and private sector performing any work in the data message format through the organisational information system lacking in confidence to make electronic transactions in all forms. Also, the Electronic Transactions Commission is aware of the necessity to promote and urge the country to be able to raise a level of competition with other countries by widely applying the information and communication system in conjunction with the electronic transactions. It is deemed important to apply various laws and regulations to the electronic transactions both on part requiring an action and on part requiring omissions in order to help the electronic transactions of a state agency to be secure and reliable.

In order to make any operation by an electronic procedure with the state agency or by the state agency secure and reliable as well as have an internationally recognised standard, the Electronic Transactions Commission deems appropriate to set the policy and practice in the Information Security of the State agency.

By virtue of Sections 5, 7 and 8 of the Royal Decree Prescribing Rules and Procedures of Electronic Transactions in the Public Sectors of B.E. 2549, the Electronic Transactions Commission issues this Notification as a preliminary guideline for state agencies to use in setting the policy and practice in the Information Security which shall at lease consist of essential substances as follows:

Clause 1 In this Notification:

(1) “User” means government official, officer, government employee, employee, system administrator, organisational executive, service recipient, general user.

(2) “Rights of the User” means general rights, exclusive rights, special rights and other rights in relation to the agency’s information system.

(3) “Asset” means any thing which is of value to the organisation.

(4) "Access or Control of Information Usage" means permission, determination of rights or authorization for the user to both electronically and physically access or use the network or information system, including permission as such for a third party and may prescribe practices regarding wrongful access.

(5) "Information Security" means confidentiality, integrity, availability of the information, including other qualifications, namely, authenticity, accountability, non-repudiation and reliability.

(6) "Information Security Event" means an event specifying the event's occurrence, service conditions or network which shows the possibility of violation of the information security policy or failed preventive measures or an event that may not know that it may pertain to the information security.

(7) "Unwanted or Unexpected Information Security Incident" means an unwanted or unexpected information security incident which may cause the organisational system to be hacked or attacked and the security to be under threat.

Clause 2 State agency shall provide a written policy in the Information Security of the agency which shall contain at least the following contents:

(1) Access or control of information usage.

(2) Providing availability of the information system and information back-up system and preparing a preparedness plan in case of emergency in an event of inability to operate by the electronic procedure so that information can be used normally and continuously.

(3) Regular audit and assessment of informational risk.

Clause 3 State agency shall provide a practice in the Information Security of the agency, which shall comprise at least the following processes:

(1) State agency shall prepare a practice which conforms to the information security policy of the agency.

(2) State agency shall notify such policy and practice to all related parties in order that such policy and practice can be accessed, understood and observed.

(3) State agency shall clearly specify a responsible person under such policy and practice.

(4) State agency shall review and improve such policy and practice to be always up-to-date.

Clause 4 Practice regarding the information security shall contain at least contents encompassing under clauses 5 to 15.

Clause 5 Requirement on the access and usage control of the information shall be provided which shall have at least the following contents:

(1) State agency shall have access control to data and equipment for processing data by taking into consideration usage and security.

(2) Regulation concerning the access authorization shall be prescribed in accordance with the policy related to permission, determination of rights or authorisation of such state agency.

(3) State agency shall specify about the category of the data, priority or hierarchy of confidentiality of the data, including hierarchy of access, time of access and channel of access.

Clause 6 Business requirements for access control shall be provided by dividing preparation of the practice into two parts, namely, information access control and improvement to correspond with the business and security requirements.

Clause 7 User access management shall be provided in order to control access to the information system exclusively for a person who has been authorised and passed an information security awareness training in order to prevent access from the unauthorised person, requiring at least the following contents:

(1) Creation of knowledge and understanding to the user in order to raise awareness and understanding to a peril and impact caused by careless or unwitting usage of the information system, including required provision of preventive measures as appropriate.

(2) User registration shall prescribe to have a practical procedure for the user registration upon authorisation to access to the information system and removal from the user registration upon revocation of such authorisation.

(3) User management shall provide control and restriction of the right to access and usage of each type of the information system as appropriate, including exclusive rights, special rights and other rights in relation to the access.

(4) User password management shall provide a strict password administration and management process for the user.

(5) Review of user access rights shall provide a process to review an access right of the information system user within the prescribed time period.

Clause 8 User responsibilities shall be prescribed in order to prevent unauthorised access, disclosure, gaining knowledge or secret copying of the information and theft of information processing equipment, which shall have the following minimum contents:

(1) Password use shall prescribe a good practice for the user in the password designation, password usage and password change with quality.

(2) Protection of the equipment while there is no user at the equipment shall prescribe an adequate practice in order to prevent a person who has no right from ability to access the equipment of the agency when a keeper is absent.

(3) Clear desk and clear screen policy shall control the informational assets, e.g., documents, computer data storage media or information not to be in a state at risk of access by a person who has no right and shall require the user to exit the information system when usage is ceased.

(4) User may apply encryption to the confidential data by complying with the Rule on Maintenance of Official Secrets B.E. 2544.

Clause 9 Network access control shall be provided in order to prevent unauthorised access of the network, which shall have the following minimum contents:

(1) Usage of network services shall prescribe that the user can gain access to the information system only of the authorized-to-access services.

(2) User authentication for external connections shall prescribe authentication before authorising an external user to enter and use the organisation’s network and information system.

(3) Equipment identification in networks shall have a procedure which can identify the equipment on networks and the equipment identification in networks shall be used as confirmation.

(4) Remote diagnostic and configuration port protection shall control both physical and network access to a port which is used for diagnosis and configuration.

(5) Segregation in networks shall be segregation in networks according to information service groups, user groups and information system groups.

(6) Network connection control shall regulate the access or usage of shared or connected networks between agencies to conform to the practice regarding access control.

(7) Network routing control shall regulate the network routing so that computers' connection and transmission or circulation of data or information shall be in line with the practice regarding access control or business applications.

Clause 10 Operating system access control shall be provided in order to prevent unauthorised access to the operating system, which shall have the following minimum contents:

(1) Determination of a procedure to enter for usage with security and access to the operating system shall be controlled by a secure authentication procedure.

(2) User identification and authentication shall require the user to have a specific data which can authenticate the user and choose an appropriate technical procedure in authentication to support a claim of being the identified user.

(3) Password management system shall be created or provided with a password management system capable of interactive or automatic junctions favorable to qualitative password designation.

(4) Use of system utilities shall be limited and controlled in order to prevent transgression or evasion of the existing or prescribed security measures.

(5) Usage of the information system shall be ceased when there is the session time-out.

(6) Limitation of connection time shall limit the connection time to make more secure for the information system or application with high risk or importance.

Clause 11 Application and information access control shall control the followings:

(1) Information access restriction shall limit or control access or entry for usage of the user and personnel supportive of entry for usage in the access of various

information and functions of the application programmes or applications to comply with the prescribed policy on information access control.

(2) System which is sensitive to interference and has an impact and high importance to the organization shall be separated from other systems and have its own specifically environmental control. Mobile computing and teleworking shall be controlled.

(3) Control of computer equipment and mobile computing and teleworking shall prescribe the appropriate practice and measure for protecting the data from risk of using the mobile computing and teleworking.

(4) Teleworking shall prescribe the procedure, plan and practical procedure for adaptation to the teleworking.

Clause 12 State agency with the information system shall create a back-up system pursuant to the following guidelines:

(1) Selection and creation of a back-up system with appropriate availability shall be properly consideration.

(2) Preparedness plan in case of emergency in an event of inability to operate by the electronic procedure so that information can be used normally and continuously shall be made by improving such preparedness plan in case of emergency to be suitably adaptable and compliant with the business usage.

(3) Duties and responsibilities of the personnel who are responsible for the information system, back-up system, and preparedness plan in case of emergency in an event of inability to operate by the electronic procedure shall be prescribed.

(4) Regular test on availability of the information system, back-up system and system of preparedness plan in case of emergency.

(5) Regarding the frequency of practice in each clause, the practice should be executed to the extent sufficient to a nature of acceptable risk of each agency.

Clause 13 State agency shall provide an information security audit and assessment with the following minimum contents:

(1) State agency shall provide the information security audit and assessment of the information system at least once a year.

(2) Information security audit and assessment shall be conducted by the internal auditor of such state agency or by an external security auditor in order for the state agency to know a level of risk and level of information security of the agency.

Clause 14 State agency shall prescribe a clear accountability in case where the computer or information system causes any damage or hazard to any one of organisation or person as a result of deficiency, neglect or violation to comply with the policy and practice in the Information Security. The chief executive who is in charge of overseeing the information of the state agency shall be responsible for the risk, damage or danger which occurred.

Clause 15 State agency may choose a practice in the Information Security which is different from this Notification if it demonstrates that the chosen practice is more appropriate or equivalent thereto.

Clause 16 This Notification shall come into force on the day following its publication in the Government Gazette.

Notified on the 31st day of May B.E. 2553

Sub-Lieutenant Ranongrak Suwanchawee

Minister of Information and Communication Technology

Chairman of Electronic Transactions Commission