Unofficial Translation

Volume 129, Special Part 191 Ngor, Government Gazette 19 December 2012

Notification of the Electronic Transactions Commission

Subject: Information Security Standards in accordance with Security Techniques

B.E. 2555

Whereas the Royal Decree on the Security Techniques in performing Electronic Transactions B.E. 2553 requires the Commission to promulgate determination of Information Security standards in accordance with security techniques in each level in order to make reliable the electronic transactions performed pursuant to the security techniques prescribed by the Commission;

By virtue of Section 7 of the Royal Decree on the Security Techniques in performing Electronic Transactions B.E. 2553, the Electronic Transactions Commission hereby issues the following Notification:

Clause 1 This Notification is called "Notification of the Electronic Transactions Commission on Information Security Standards in accordance with Security Techniques B.E. 2555".

Clause 2 In case of a requirement to act in compliance with Information Security Standards in accordance with the Security Techniques in a strict, medium or basic level, the agency or organization or divisions of the agency or organization shall comply with the Information Security Standards in accordance with prescribed rules attached to this Notification.

Clause 3 This Notification shall come into force after three hundred and sixty days from the date of its publication in the Government Gazette.

Notified on the 13th day of November B.E. 2555

Group Captain Anudith Nakornthap

Minister of Information and Communication Technology

Chairman of Electronic Transactions Commission

Volume 129, Special Part 191 Ngor, Government Gazette 19 December 2012

Schedule Attached to the Notification of the Electronic Transactions Commission
Subject: Information Security Standards in accordance with Security Techniques B.E. 2555

Information Security standards are measures for use in regulation to afford security to the information system, which covers confidentiality, integrity and availability of the information system and information in such system. Performance of electronic transactions through the information system shall be undertaken in accordance with related measures pursuant to the attached schedule, and shall consider being in alignment with the level of risks derived from the assessment. The Information Security standards are divided into the following 11 clauses:

1. Formation of administrative security;
2. Arrangement of the information security structure in an information security administration section both inside and outside the agency or organization.
3. Administration of information assets;
4. Formation of information security on human resources;
5. Formation of physical and environmental information security;
6. Administration of communications and operations of the computer network system, computer system, computer function system and information system;
7. Control of access to the computer network system, computer system, computer function system, information system, information, electronic messaging and computer data;
8. Procurement or provision of development and maintenance of the computer network system, computer system, computer function system and information system;
9. Administration of unwanted or unforeseen security situations;
10. Administration of services or operations of the agency or organisation to ensure continuity; and
11. Audit and evaluation of compliance with any policies, measures, rules or processes, including the information security requirements.

1. Information Security Standards In accordance with the Basic Level of Security Techniques

Information Security standards in accordance with the basic level of security techniques shall be performed as follows:

Clause 1 Formation of administrative security, an agency shall prescribe the information security policy going through approval and push by a high-level executive; and such policy shall be announced to the employees and third parties concerned for their acknowledgement.

Clause 2 Arrangement of the information security structure in an information security administration section both inside and outside the agency or organization.

2.1 A high-level executive of the agency shall be responsible for the information works of the agency, furnish support and set a clear direction of operations regarding the information security, including clear assignments of relevant works to practitioners as well as being accountable for any risk, damage or peril which occurs to the information system in any event whatsoever.

2.2 Regarding the new information system, a review procedure shall be prescribed by which to authorize the formation, installation or usage in various aspects, such as administration of system subscribers or a capacity to function compatibly between the old system and the new system.

2.3 Confidentiality agreement or non-disclosure agreement which aligns with the situation and needs of the agency in safeguarding information shall be prescribed.

2.4 Requirement concerning the information security for authorizing the subscribers who are a third party to gain access to the information system or use information of the agency shall be incorporated.

2.5 Regarding an agreement to permit the third party's access to the information system or use information of the agency for reading, processing, administrating of information system or developing of information system, there should be a requirement with respect to the information security in the agreement.

Clause 3 Administration of information assets shall entail archiving of information assets, whereby the archived data shall compose of data necessary for searching for subsequent usage.

Clause 4 Formation of information security on human resources

4.1 Determination of the hired employee's, agency's or third party's obligations and responsibilities to align with the information security and the policy on the information security promulgated by the agency.

4.2 The high-level executives of the agency shall direct that the hired employee, agency or third party performs work in accordance with the policy or regulation on security promulgated by the agency.

4.3 Determination of the procedure to punish an employee who violates the policy or regulation regarding the information security in the agency.

4.4 Clear determination of obligations and responsibilities in terminating employment or changing the employment status, and clear assignment of the responsible person.

4.5 The hired employee, agency or third party shall return the information assets of the agency upon termination of his/her employment status, or upon the expiration of his/her contract or agreement to work for the agency.

4.6 Cancellation of the rights of the employee, agency or third party to access for use of the information system shall be executed upon termination of his/her employment status, or upon the expiration of his/her contract or agreement to work and appropriate alteration of the level of rights to access for use of the information system shall be executed when there is any change of obligations and responsibilities that have been arisen.

Clause 5 Formation of physical and environmental security

5.1 Protection of the security perimeter in which there exists installation, archiving or usage of the information system and information shall be carried out.

5.2 Physical security protection shall be designed and installed in order to prevent external perils and those in a catastrophic degree, whether caused by a human being or a natural disaster, such as fire, flood, earthquake, explosion, riot etc.

5.3 Information equipment shall be positioned and protected in order to reduce a risk from various natural disasters or dangers, and prevent the unauthorised access.

5.4 Information equipment shall be protected from probably the power failure or interruption caused by mistakes of supporting utilities.

5.5 Information equipment shall be taken care of in a correct manner in order to continue its accuracy and integrity and remain constant availability.

Clause 6 Administration of communications and operations of the computer network system, computer system, computer function system and information system.

6.1 Document on the working procedure shall be prepared, improved and cared for availability, thus enabling the employee to apply such document in practice.

6.2 Outsourced person or agency which provides hired services to the agency shall be supervised to comply with the servicing contract or agreement as specified, which shall cover the security work, character of servicing and degree of servicing.

6.3 Reports or records of services rendered by the outsourced person or agency which provides services to the agency as hired shall be regularly monitored and examined.

6.4 Criteria for inspection of an upgrade or new version of information system shall be made available and an information system test should be conducted both in a period of system development and pre-inspection.

6.5 Procedure for control of the audit, protection and recovery in an event of unwanted usage of the program and creation of awareness to subscribers of the information system relating to any unwanted program shall be provided.

6.6 Back-up information and a re-application test which shall meet the data back-up policy announced by the agency shall be provided.

6.7 Administration of the computer network control to prevent threats and Information Security and applications which function on the computer network, including the information exchanged on such network, shall be provided.

6.8 Determination of the form of security, degree of servicing, requirements on administration in the computer network servicing agreement whether it be services provided by the agency itself or subcontracted to the outsourced service provider shall be provided.

6.9 Policy and working procedure, including control of information exchange through a channel of communication in electronic messaging format shall be provided.

6.10 Agreement regarding exchange of information or software between the agency and the outsourced person or agency shall be provided.

6.11 Policy and working procedure to protect information which is communicated or exchanged through the information system linked with various information systems shall be provided.

6.12 Protection of information which is exchanged when performing the electronic commerce through a public computer network in order to prevent fraud, contractual breach, or leakage or unauthorised alteration of information shall be provided.

6.13 Protection of information which is communicated or exchanged when performing the online transaction in order to prevent incomplete data reception and transmission, or transmission of data to a wrong place, or data leakage or unauthorised data alteration, reproduction or re-transmission shall be provided.

6.14 For information disseminated to the public, prevention of unauthorised alteration shall be provided in order to preserve integrity of the information.

6.15 Audit log which records data on usage activities of the information system subscribers and security-related incidents for the purpose of investigation in the future and tracking control of access shall be provided.

6.16 Monitoring procedure to observe usage of the information system and constant evaluation follow-ups of such monitoring to observe shall be provided.

6.17 Protection of the information system which stores log and log data in order to prevent unauthorised access or alteration shall be provided.

6.18 Log which relates to maintenance of the information system by a system administrator or system operator shall be stored.

Clause 7 Control of access to the computer network system, computer system, computer function system, information system, information, electronic messaging and computer data.

7.1 Documentary access control policy and a follow-up review of such policy to ensure alignment with the requirements or needs on the operation or provision of services and information security shall be provided.

7.2 Registration of a subscriber account of the information system shall be provided and the subscriber account shall be officially cancelled in order to regulate granting of the right and cancellation of the right to enter and use any information system of the agency.

7.3 Determination of the right to access in a high-level shall be restrictively executed and under supervision.

7.4 The Subscriber shall take care and protect any information equipment under the caring responsibility during the non-usage period.

7.5 Access to the agency's computer network capable of external access shall be restricted, which must align with the access control policy and requirements of application usage for operation.

7.6 All Subscribers shall have their own subscriber account and the information system shall embody a sufficient identification technique to enable identification of the information system subscriber.

7.7 Automatic shutdown or close of the information system usage screen if there is no usage exceeding the prescribed maximum period.

7.8 Access to various information and functions in the applications of the information system subscriber's and administrator's shall be confined in order to align with the prescribed access policy.

7.9 Policy and guidelines on security administration to lower the risk in the usage of information equipment or mobile communication equipment such as a laptop computer or smart phone, etc. shall be prescribed.

Clause 8 Procurement or provision of development and maintenance of the computer network system, computer system, computer function system and information system.

8.1 In preparation of the minimum requirements of the new information system or improvement of the original information system, a requirement on the control of information security shall be set out.

8.2 Care, control and monitoring for inspection of the work done in subcontracting the software development.

Clause 9 Administration of unwanted or unforeseen security situations shall be provided in which the unwanted or unforeseen security situations shall be reported via the appropriate administrative channel as soon as possible.

Clause 10 Administration of services or operations of the agency or organisation to ensure continuity shall be carried out by prescribing a plan for maintaining or recovering provision of information service after the event giving rise to interruption of operation, whereby availability of the information in accordance with a specified level within the prescribed time period is provided.

Clause 11 Audit and evaluation of compliance with any policies, measures, rules or processes, including the information security requirements.

11.1 Guidance in operation of the information system that aligns with the laws and contractual requirements of the agency shall be clearly specified, documented and always updated.

11.2 Information system shall be prevented from usage for the wrong purpose.

11.3 An employee of the agency shall ensure that the works relating to information security within a scope of responsibility will be operated in alignment with the laws and contractual requirements of the agency.

2. Information Security Standards In accordance with the medium Level of Security Techniques

The Information Security standards in accordance with the medium level of security techniques shall follow Information Security standards in accordance with the basic level of security techniques, and shall have the following additional compliance:

Clause 1 Regarding administrative security formation, the agency shall set up a follow-up and evaluation plan of information security usage and the regular

Information Security policy for improvement if there are any changes inside the agency to suit the situation of usage and remain constant effectiveness.

Clause 2 Arrangement of the information security structure in an information security administration section both inside and outside the agency or organization.

2.1 Content of works or various obligations and responsibilities regarding the information security shall be prescribed.

2.2 Procedure and channel for communication with the outsourced agency with specialised expertise or the agency which expertise on information under various circumstances shall be clearly prescribed.

2.3 Consideration for review of the guidance in the administration regarding information security shall be regularly provided or when there is any change in the operation, provided that such consideration for review should be conducted by a person with no interest in the works subject to the consideration for review.

Clause 3: Administration of information assets.

3.1 Person with a duty to monitor usage control and bear responsibility for the information assets shall be determined.

3.2 Rules for the usage of information assets shall be imposed, documented and announced inside the agency.

3.3 Categorization of information shall be provided by classifying according to the information value, legal requirements, hierarchy of confidentiality and importance to the agency.

3.4 Use of the appropriate procedure in categorizing and managing information shall be prescribed and announced in alignment with the categorization guideline announced by the agency.

Clause 4 Employee, outsourced agency or person shall receive training on formation of information security on human resources in order to generate awareness relating to information security on the part involving his/her responsibilities and regular communication of the policy or rule of practice on information security that the agency announces, or when there is any change thereof.

Clause 5 Formation of physical and environmental security.

5.1 Protection of physical security shall be designed and installed in order to safeguard the area or workplace or various information equipment.

5.2 Information equipment, information or software should not be removed out of the agency's workplace without permission.

Clause 6 Administration of communications and operations of the computer network system, computer system, computer function system and information system.

6.1 Changes of the information system shall be managed and controlled.

6.2 Follow-ups on usage of the information assets and planning of information assets shall be provided in order to suitably support future performance.

6.3 Working procedure in administration and archiving of the information shall be provided in order to prevent information from leakage or use in the wrong purpose.

6.4 Log relating to any errors of the information system shall be stored, such log shall be regularly analyzed, and detected errors shall be suitably rectified.

6.5 Synchronization of the time system of various information systems used in the agency or security domain shall be provided by setting a value together with time from a dependable source of time.

Clause 7 Control of access to the computer network system, computer system, computer function system, information system, information, electronic messaging and computer data.

7.1 Regulation on a procedure for choosing a password with security as prescribed by the agency with which the Subscriber must comply shall be provided.

7.2 Subscriber can access to services through the computer network which the Subscriber has been authorised to use only.

7.3 Sufficient identification technique shall be prescribed in order to control remote access to the agency's information system.

7.4 Control of access to the channel of maintaining the information system both physically and connection through the computer for the information system

which can be remotely accessed, such as, remote diagnostic or configuration facility of the computer network equipment.

7.5 Grouping in accordance with categories of information to which services are rendered, information system, group of subscribers shall be provided by separating in proportion on the computer network.

7.6 Control of the information flow route in the computer network system shall be prescribed in order to prevent conflict with the access control policy of the applications.

7.7 Log-on procedure shall be prescribed in order to control access to the computer operating system.

7.8 Password administration system which can function in an interactive manner with the subscriber and support the secure password usage shall be established or provided.

Clause 8 Procurement or provision of development and maintenance of the computer network system, computer system, computer function system and information system.

8.1 Any data which is accepted into the applications shall be always validated first in order to ensure that the data has correctness and appropriate format.

8.2 Any data which results from processing of applications shall be validated in order to ensure that the data derived from the processing is correct and appropriate.

8.3 Key management guideline shall be provided in order to support technical usage which relates to the agency's encryption.

8.4 Information set which will be used for testing in the information system shall be carefully selected, including having a guideline on control and prevention against leakage of data.

8.5 Access to the program's source code shall be restricted.

8.6 If there is any change in the computer operating system, the function of the crucial program shall be inspected, reviewed and usage shall be tested in order to ensure that the result of such change will not cause any impact on the agency's information security and services rendered.

Clause 9 Administration of services or operations of the agency or organisation to ensure continuity.

9.1 Requirement relating to the necessary information security shall be provided by being specified as part of the administration procedure for continuous operation during an emergency situation.

9.2 Main framework for development of the administration plan for continuous operation during the emergency situation shall be prescribed to ensure that various developments are moving in the same direction, including alignment with the security requirement, as well as prioritization in order of importance in the test and maintenance.

9.3 Administration plan for continuous operation during an emergency situation shall be tested and adjusted to ensure that such plan is always up-to-date and effective.

Clause 10 Audit and evaluation of compliance with any policies, measures, rules or processes, including the information security requirements

10.1 Protection of personal information which aligns with the laws and requirements under various contracts of the agency shall be provided.

10.2 Technique for encryption which aligns with the laws and requirements under various contracts of the agency shall be applied.

10.3 Technical part of the information system shall be regularly reviewed and inspected in order to align with the development standard of information security work.

10.4 Audit requirement and activities related to the audit of the information system shall be planned and established in order to decrease the risk in existence of interruption to provide services.

10.5 Access to use the equipment employed for the audit shall be protected in order to prevent any usage in the wrong purpose or the usage from being violated (Compromise).

3. Information Security Standards In accordance with the Strict Level of Security Techniques

The Information Security standards in accordance with the strict level of Security Techniques shall follow the Information Security standards in accordance with the basic and medium level of Security Techniques, and shall have the following additional compliance:

Clause 1 Arrangement of the information security structure in an information security administration section both inside and outside the agency or organization.

1.1 Collaboration between the people playing roles associated with the information security of the agency in any work or activities relating to the information security shall be established.

1.2 Procedure and channel in communicating with the outsourced agency with a supervisory duty or a law enforcement agency, including the agency monitoring emergency situations under various circumstances shall be clearly prescribed.

1.3 Prior to authorising the outsourced agency or person to gain access to the information system or use the information of the agency, the potential risk shall be specified and preventive guidance to minimize such risk shall be determined before authorisation.

Clause 2 Formation of information security on human resources.

2.1 In considering for recruitment of employees or hiring of the outsourced agency or person, the history or qualifications shall be verified in order to ensure compliance with relevant rules and ethics which shall take into account the hierarchy of confidentiality of the information to be accessed and the assessed level of risk.

2.2 In the employment contract or performance agreement of the employees or the hiring agreement of the outsourced agency or person, obligations and responsibilities on the information security shall be specified in the agreement.

Clause 3 Formation of physical and environmental security

3.1 In the secure area, access and exit shall be regulated and granted only to persons who are authorised to access and exit.

3.2 Physical protection guideline for working in the secure area shall be designed and such use shall be prescribed.

3.3 Areas accessible by persons not qualified to access such as the delivery point etc., shall be controlled, or if possible, such area shall be separated from the installation, archiving or used area of the information system and information in order to avoid unauthorised access.

3.4 Cable used for communication or wires shall be prevented from interception or occurrence of damage.

3.5 Security given to the information equipment which is used outside the workplace of the agency shall be maintained by taking into consideration different levels of risk from usage in various places.

3.6 Prior to cancellation of usage or distribution of the information equipment, such information equipment shall be checked whether there has been any deletion, moving, or destruction of significant data or procured and installed software by irrecoverable means.

Clause 4 Administration of communications and operations of the computer network system, computer system, computer function system and information system

4.1 Duties and scope of responsibilities shall be clearly separated in order to reduce the chance of errors in the change or usage of the information system or information for the wrong purpose.

4.2 Information system for development, testing, and actual use shall be separated from each other in order to lower the risk in unauthorised access for usage or alteration of the information system.

4.3 Any change relating to preparation for providing services and improvement of the information security policy, performance procedure, or control regarding the information security shall be administered and managed by taking into account the degree of importance of related business operations and continuing risk assessment.

4.4 If the agency allows usage of a mobile code (such as a certain script of the web application which automatically functions upon web browsing), configuration

should be set in order to ensure that the mobile code operations satisfy both the information security and security policy and the mobile code operations in the information system should be automatically prohibited if a category of such mobile code is forbidden from functioning in the information security policy.

4.5 Performance procedure for the administration of a removable media shall be provided.

4.6 Performance procedure in destructing the securely removable media shall be provided.

4.7 Data or system documentation shall be protected from unauthorised access.

4.8 In case of moving of equipment which archives the information, the equipment used for archiving such data shall be protected from unauthorised access or usage in the wrong purpose, or damage to the equipment or information.

4.9 Information communicated through the electronic messaging, such as, electronic mail (E-mail), EDI or Instant messaging.

Clause 5 Control of access to the computer network system, computer system, computer function system, information system, information, electronic messaging and computer data

5.1 Administration procedure with regard to determination of an official password shall be provided.

5.2 Requirement on the executive to keep track of and review the subscriber's level of right to official access shall be regularly imposed.

5.3 Clear desk policy shall be prescribed for information in paper form and that archived in the removable media and the clear screen policy for the information system.

5.4 Automatic equipment identification shall be specified in order to audit the connection of such equipment as to whether it is actually from such equipment or from a specified place only, thus necessitating the information system to receive connection exclusively from the authorised equipment or authorised place.

5.5 Access for usage of various utility programs shall be strictly restricted as such program may have the capacity to monitor and change operations of the information system.

5.6 Time period for connection with a high-risk information system shall be confined in order to increase the security level.

5.7 For the information system with high importance, the information system shall be operated in a separate environment without mixing with other information systems.

5.8 Policy, plan and procedure of performance associated with teleworking activities.

Clause 6 Procurement or provision of development and maintenance of the computer network system, computer system, computer function system and information system.

6.1 Operations of applications to detect data errors which may result from the working or processing errors shall be validated.

6.2 Minimum requirement for keeping authenticity and integrity of the data in the application, including determination and compliance with the appropriate protective means shall be provided.

6.3 Policy on technical usage which relates to encryption shall be provided.

6.4 Performance procedure shall be provided in order to control the software installation on the information system services.

6.5 Control of various changes in developing the information system with the official control procedure shall be provided.

6.7 Any changes to the software package shall be confined to only necessary changes and every change shall be strictly regulated.

6.8 Protective measures to reduce chance of the information leakage shall be provided.

Clause 7 Administration of unwanted or unforeseen security situations.

7.1 Employee or subscriber who is a third party shall be required to record and report any weak points which may be observed during the information system's usage.

7.2 Scope of responsibilities of the executives and performance procedure shall be prescribed in order to promptly, orderly and effectively respond with the unwanted or unforeseen security situations.

7.3 If in the follow-up procedure with the person or agency after occurrence of the unwanted or unforeseen security situations involving legal proceedings (whether civil or criminal), collection, storing and presentation of the evidence shall be provided in alignment with the rules of the law in force.

Clause 8: Administration of services or operations of the agency or organisation to ensure continuity shall comprise specification of any event which may result in interruption of operation and possibility of an impact to occur, as well as a consequential effect from such interruption in terms of the information security.

Clause 9: Audit and evaluation of compliance with any policy, measure, rule or process, including the information security requirement.

9.1 Performance procedure shall be defined in order to ensure that usage of the data which may be deemed as intellectual property or usage of software shall be in alignment with the laws and requirements under various agreements.

9.2 Important information shall be protected from damage, loss or forgery by corresponding with the laws, requirements under various agreements of the agency, and the servicing requirements.