Regulation of Thailand Institute of Scientific and Technological Research on

Information Security Management

B.E. 2560 (2017)

Properly, the criteria and procedure of information security management has been defined for carrying out information security system continuously and effectively. The business could perform integrity and staffs could perform legally, harmonizing the Standards of Security in Electronic Transactions and verify the Computer-related Crime Act B.E 2550 (2007) and revision.

Refer to section 26 (6) in Thailand Institute of Scientific and Technological Research Act B.E. 2560, the Governor of the Thailand Institute of Scientific and Technological Research has laid down the regulation as following.

Clause 1. This regulation is called "Regulation of Thailand Institute of Scientific and Technological Research on Information Security Management B.E. 2560"

Clause 2. This regulation is enforced from the date of announcement.

Clause 3. Cancelling the Regulation of Thailand Institute of Scientific and Technological Research on Information Security Management B.E. 2559 and all regulations and rules contrary to this regulation and use this regulation in place.

Clause 4. In this regulation;

“Institute” means Thailand Institute of Scientific and Technological Research;

“Governor” means the Governor of Thailand Institute of Scientific and Technological Research;

“Chief Information Officer” means executor appointed from the Governor and has authorization in information technology and communication of the Institute, his role and duty in defining the policy and standard to control information technology system and communication;

“Information system” means safe system, computer system, work system, database system, network system, system user, system programmer, system manager and executors in all agencies, all components work together to define the objectives, storage data, compile data result and transmit output or information to system user or executors for support the opeation, decision, planning, execution, control, analysis and evaluation of the agency in each level in the Institute.

"Computer system" means set of computer and accessory including equipment for storage, transmit the data, printing the data, backup data, link data with other equipment, and including program and database program system, application program and all types of program linking to work together.

"Work system" means process o working of the agency to study, analysis, design and create using information technology, and computer and accessory, supporting program appropriately and effectively. It could solve the problem of old work process and could storage data systematically, be compiled rapidly, correctly and safety.

"Database system" means set of computer an accessory including data and database program for storage data systematically, design of structure for managing the complicated, contrast, cause the data reliability and safety.

"Network system" means linkage of computer more than two computers for communication, transmission of data, information among the computers for linkage to work together both intranet and internet.

"Internet" means big computer network system link to many network system worldwide for service of transmission of data, information between the users by using specific technology.

"E-mail system" means letter system that person used in transmission through internet.

"System Administrator" means director of the Digital and Information Division or appointed officer to take care of the information system of the Institute.

"System User" means Governor, officer, employee, appointed person according to the contract, agreement, or invoice and outsider submitted to access and use the information system of the Institute.

"Password" means letter or numerical code composed into set which the system administrator or computer system or system user defined for authenticated for access into the information system.

"Virus" means set of command or program intruded into computer or accessory and distributed into the information system, obstruct to work or damage data of information.

"Virus Protection Program" means computer program which detect and remove virus, it must be legal and could be improve program and remove new virus.

"Security" means procedure to make the information system as the basic 3 properties as the following;

(1) Confidentiality is keeping data confidentially and only the right person could access the data;
(2) Integrity is to verify data not be taking action that cause change or alter from illegal person, intentionally or not;
(3) Availability is to verify that data or information system ready to service when the request to use.

Clause 5. The Governor is acting as in this regulation;

In case there is problem in this regulation, Governor is the person to consider and the consideration is finalized.

Part 1

Condition for Access to Work System and Password Use

Clause 6. The system user must define the password and take of his password as the criteria of system administrator defined and must permit system administrator to carry out for the security of the information system.

Clause 7. The system user must keep and conceal his password, not leak to others and do not inform to any person. In case the authorized could not work, the representative must be replaced.

Clause 8. In case do not use information system, system user must log out the system at once to prevent the leak, if suspect there would be the leak, change the password at once.

Clause 9. Prohibit the system user without permission access into the information system in every case.

Part 2

Virus protection

Clause 10. The system user must take care of computer used in information system and installed virus protection program.

Clause 11. The system user do not bring illegal program or data media such as CD, DVD, flash drive using with other computer or suspected source of data without inspection and removal of virus.

Clause 12. The system user must not download data or program not relating to the work or website unreliability or not safety.

Part 3

Use of Computer Safety to Information System

Clause 13. Do not install other software or program into the computer or install accessory link to network or link with personal computer to connect with the network of the Institute except have the permission from the system administrator.

Clause 14. The system user must not reveal or share file in the computer except the work system that the Institute defined. If necessary, the time limit of work, and cancel at once finish work for preventing the damage that may happen to the computer system and data.

Clause 15. The system user must backup the data.

Part 4

Performance according to Computer-related Crime Law

And Use of Internet System

Clause 16. The system administrator must register computer link to Institute's network system that could authenticate where it is located in the institute.

Clause 17. The system user must register to be system user by given the access right and password as the tool in authentication to access the network of the Institute. Each user must take care of right to use his password, do not permit anyone to use his password. If it is found that fault from Electronic Transactions Act, the ownership user must be responsible for the damage happened without deny.

Clause 18. The system user must not use internet system in multimedia data or download big file irrelevant to work and occupy a lot of data communication symbol channel.

Clause 19. The system user must use official or Institute e-mail system for officially or work.

Part 5

Policy and Procedure in Information Security

Clause 20. For the Institute has carried out to respond the Computer-related Crime Law and Royal Decree Prescribing Rules and Procedures for Electronic Transactions in Public Sector B.E. 2549 and the Electronic Transactions Act B.E. 2544 and revision (second version) B.E.2551 and the procedure guide line for officer and employee to perform. It aims to reduce risk from threats in information technology and communication both inside and outside organization, including create the reliability, integrity, security, validation and personal to stakeholders, system user, and customer. The Institute defines the policy and procedure in information security of the Institute in written and announce to system user, relevant person to know and perform, including review, improve policy regularly for perform integration.

Clause 21. The Institute or appointed agency is the inspector of risk assessment in information security management at least once a year. And have the duty to report the situation for security risk to committee in information security for improving system more security.

Clause 22. The Institute or appointed agency provide the activity for create the awareness of knowledge, understanding to information system user correctly, properly and safety.

Clause 23. The committee on information security comprises of chief information officer as the chairman, executors and officers as the committee, and director of Digital System Division as the committee and secretary. The committee has the role to review, improve and provide the policy and procedure on information security as appropriate at least once a year.

Clause 24. The Institute or appointed agency review procedure of information security management as appropriate at least once a year.

Notified on date of 29th March B.E.2560.

(Mrs. Luxsamee Plangsangmas)

Governor