THAILAND INSTITUTE OF SCIENTIFIC AND TECHNOLOGICAL RESEARCH

Notification

of Thailand Institute of Scientific and Technological Research's

Information Security Policy and Procedure B.E. 2560 (2017)

At present, the information security threat has been increased continuously and tends to impact to both private sector and government sector. It causes entrepreneur and government organization and private organization carrying out electronic data through organization information system create confidence in all types of electronic transaction. At present, it is necessary to use information system and communication application in electronic transaction. The law, regulations in electronic transaction to do or refrain must be aware and important. This is for being the direction and support organization information security with harmonizing to the business and legal principles reliability and in standard. The Chief Information Officer, CIO and Chief Executive Officer, CEO of Thailand Institute of Scientific and Technological Research would be controller, and be responsible for damage risk or danger that may happen in case the damage or danger of information system to Thailand Institute of Scientific and Technological Research or any person due to fault, avoid or infringe to carry out according to Thailand Institute of Scientific and Technological Research's Information Security Policy and Procedure. And the director of the Digital and Information Division is responsible for controlling securing the performance according to Thailand Institute of Scientific and Technological Research's Information Security Policy and Procedure. And Thailand Institute of Scientific and Technological Research's Information Security Policy and Procedure would be reviewed and updated, therefore Thailand Institute of Scientific and Technological Research's Information Security Policy and Procedure has been defined as the following.

Section 1. This notification is called "Notification of Thailand Institute of Scientific and Technological Research's Information Security Policy and Procedure B.E. 2560".

Section 2. Cancelling the Notification on TISTR's information security policies dated 11th September B.E. 2555, and cancelling any notifications or any orders that has been defined in this notification or contrary to this notification. This notification is used in place.

Section 3. This notification enforces the officers, employees and executors concerning information system. It includes the outsiders regarding the Thailand Institute of Scientific and Technological Research's information system.

CHAPTER 1

General

Section 4. This notification is provided in harmonization with the Rule on Thailand Institute of Scientific and Technological Research's Information Security B.E. 2560 (2017), and for defining the information security policies and procedure, for harmonizing Thailand Institute of Scientific and Technological Research's policies and mission consisting of the following policies;

(1) Acceptable Use Policy;
(2) Physical and Environmental Security;
(3) Assess Control Policy;
(4) Network and Server Policy;
(5) Wireless Policy;
(6) Firewall Policy;
(7) E-mail Policy;
(8) Internet Security Policy;
(9) Intrusion Detection System/Intrusion Prevention System Policy: IDS/IPS Policy;
(10) Backup Policy;
(11) Database Security Policy.

Section 5. In this notification;

"**Institute**" means Thailand Institute of Scientific and Technological Research;

"**User**" means executors, officers and employees concerning information system including outsiders regarding the Thailand Institute of Scientific and Technological Research's information system.

"**System Administrator**" means a person assigned by the director, is responsible for maintain or manage any part of computer system and network system.

"**User Right**" means general right, special right, and any right concerning information system, the agency would consider the property use right.

"**Agency**" means the Institute and agency in the Institute.

"**Information Asset**" means

1. Network system, computer system and information system;
2. Computer, accessory, recorder and mobile wireless accessory with connect to the network such as telephone, network accessory etc.;
3. Information data, electronic data and computer data.

"**Information System**" means

1. Computer System;
2. Communication System;
3. Information carried out in computer system and network system.

"**Computer System**" means computer accessory or accessory set which connect together by defining the order, order set or any and performance guideline for accessory or accessory set for compiling data automatically.

"**Communication System**" means the system comprising of receiver, sender and media for data transmission (letter, numerical code, picture, sound etc.) both wire circuit system such as coaxial cable, fiber optic, shielded and unshielded twisted pair cable, and wireless system such as microwave, satellite including other accessory such as hub, switching and router.

"**Information**" means the facts from data screening through compiling which may be in the digital, message or graphic form that user could understand easily such as report, table, chart etc. and be able to use in administration, planning, decision and other.

"**Network System**" means the system that could communicate or transmit the data and information among various information technology system such as LAN system, Intranet system, Internet system etc.

1. LAN System and Intranet System means electronic network system connecting to various computer system in the same office. The network has the objective to data communication and exchange within the office.

2. Internet System means electronic network system connecting to various computer system with worldwide internet network.

"**Information Technology System**" means office work system using information technology, computer system and network system to assist information creation for utilizing in planning, executing, support the services, development and control of communication. It comprises of computer system, network system, program, data and information, etc.

"**Computer**" means desktop computer and notebook computer.

"**Computer Data**" means data, massage, command, command set or any matter in the computer system in the condition that computer system could compile and it includes electronic data as in the law for electronic business.

"**Information Access or Control**" means the permission, right definition or empower the user to access or use the network or information system both in electronic and physical, it includes the permission for the outsiders and the performance for illegal access may be defined.

"**Information Security**" means the maintenance of confidentiality, integrity and availability of information including other properties such as correctness, non-repudiation, and reliability.

"**Password**" means letter or numerical code used as a tool in identification for data access control in data and information technology system security.

"**Risk**" means the opportunity to happen the errors, damages, leak, loss or undesirable situation.

"**Risk Assessment**" means the process to analysis of threats and weakness of information system including the impacts from information loss or loss of ability to maintain information security. The risk assessment is used as the fundamental to set out the appropriate security measures for information system.

CHAPTER 2

Information Security Policy and Procedure Guideline

Part 1

Acceptable Use Policy

Accountability, Identification and Authentication

Section 6. The user is responsible for protecting and securing username and password. Each user has his own username, prohibiting to use the username with other person, and distributing the password to others.

Section 7. The user has to be responsible for any performances happening from username, in case that user has done or not.

Section 8. The user has to set the password for security which the password comprises of not less than 8 letters comprising numerical character, alphabet or special character.

Section 9. The user has to change the password every 90 days or every time whenever being informed for changing the password.

Section 10. The user has to carry out authentication every time before using the asset or information system of the Institute. If the authentication is found the problem of password or locking or any error, the user has to inform the system administrator at once.

(1) All types of computer before access into the operating system, it must be authenticated every time;

(2) Other computer use in network has to be authenticated every time;

(3) Using internet has to authenticate and account which could identify the user;

(4) When the user is not at the computer, the user must lock screen every time, and has to authenticate before using every time;

(5) All computer must set timing for screen saver at least 5 minutes. Between leave out for lunch and after working time, the user should log out the computer;

(6) The user should allow others to use his own username and password to access the computer together.

Assets Management

Section 11. The user must not enter into the server room of the Institute where is the restricted area except for having the permission from the system administrator.

Section 12. The user must not bring accessory or any part out of the server room except for having the permission from the system administrator.

Section 13. The user must not bring the equipment or any accessory connecting to the network for doing business.

Section 14. The user must not use or delete other files in any case.

Section 15. The user must not copy or make a copy of copyright file before permission.

Section 16. The user must be responsible for the Institute asset like user's asset. The asset lists would be in the attachment of this notification. The asset return would be recorded and checked every time by assigned officer.

Section 17. In case of working out, the user must maintain and be responsible for the Institute asset as to the assignment.

Section 18. The user is responsible for the damage in case of ruin or loss as the value of the asset, if the damage is caused by the careless user.

Section 19. The user must not allow the others to use the computer or notebook in any case, except for the authoritarian has written approved.

Section 20. The asset and various information system that the Institute has provided for the objective of the Institute work only. The user is not allowed to bring any the asset or various information system using in the activities that the Institute does not define or causes any damage to the Institute.

Section 21. Any damage caused from infringe as in section 20 is individual mistake. The user has to be responsible for the damage.

Corporate Management

Section 22. The user must be aware of data use both the Institute's data or the other data.

Section 23. The data in the information asset of the office are owned by the Institute's asset. Do not permit to distribute, change, duplicate or ruin with the permission from superior or assigned agency from the Institute.

Section 24. The user has the participation in maintaining and being responsible for the Institute's data or customer's data. If the damage by illegal use, distribution without permission, the user has to be responsible for those damage.

Section 25. The user must protect and secure confidentially, integrity and availability.

Section 26. The user has the right to secure and protect personnel data properly. The Institute would encourage and respect individual right, do not permit any person to infringe individual data without permission from user occupied the data. Exception that the Institute wants to data audit or relevant to the Institute. The Institute may set out the auditor to those date without informed user.

IT Infrastructure Management

Section 27. Any program and hardware development must not perform in the following;

(1) Develop any program or hardware to destroy the mechanism of the security system, including the password is hiding used, stealing to make a copy of other data, or copy other password;

(2) Develop any program or hardware that the user has the right and prioritize to occupy the system asset more than others;

(3) Develop any program to repeat the program, or hide the program with other program as the snail or computer virus;

(4) Develop any program or hardware to destroy software license system;

(5) Present illegal data, breaking copyright, inappropriate pictures or immoral and tradition of Thailand, in case of user create the webpage on computer network.

Section 28. Do not open or run Peer-to-Peer program or risk program in the same level such as Bittorrent, except the superior has permitted.

Section 29. Do not open or run all types of online program for amusement such as television watching, music listening, games etc. during working time.

Section 30. Do not use all types of asset and communication system and the Institute's accessory to distribute data, message, picture or any matter which is immoral and security of the country, law or impact to the Institute mission.

Section 31. Do not use all types of asset and communication system and the Institute's accessory to disturb, damage and steal the data which is illegal and immoral or impact to the Institute mission.

Section 32. Do not use all types of the Institute's asset for trade benefit;

Section 33. Do not do anything to trap the data, such as message, picture, sound or any matter in the Institute's network. Exception the performance is carried out for weakness finding or system security test with the permission of system administrator.

Section 34. Do not do anything to disturb, damage or cause the Institute's information system hang.

Section 35. Do not use the Institute's information system to control other information system without the permission from the authoritarian.

Section 36. Do not perform as stealing the other password in any case for access the data or asset use.

Section 37. Do not install accessory or any performance in order to be able to access the office information system without permission from the authoritarian.

Information Security Management

Section 38. Set out and improve in policy and procedure guideline for information system regularly at least once a year.

Section 39. Intend or communicate to all staffs to give precedence to perform as the security policy strictly and regularly.

Section 40. Set out the meeting on security management regularly at least once a year. The agenda of the meeting should be at least the following;

(1) Audit the performance so as to the security policy and audit result;

(2) Action plan for protection/resolving from the audit result;

(3) Improvement of security policy next year;

(4) Risk assessment and risk reduction plan including providing asset in personnel, budget, administration and raw material sufficient for such management.

Section 41. Set out the creation of awareness in security for staffs in organization to understand and have knowledge and protect early at least once a year.

Section 42. Provide the risk assessment for information technology at least once a year, provide to set out the risk reduction plan or finding problem.

Section 43. Provide to audit the performance in security policy by internal auditor at least once a year. And it provide the plan for improvement or finding problem.

Section 44. Provide to circulate to all staffs to be careful and secure the asset that he uses for protection loss at least once a year.

Section 45. Specify policy for utilizing network system, not permission to use such as watching movie through internet etc. including internet improvement as necessary. The policy in using network system consists of the following;

(1) Do not access the types of web side in the following;
    a. Commend about the national, religion and the King;
    b. Pornography;
    c. Bet and illegal relation and immorality;
(2) Do not play games, movie watching during the working time.

Software Licensing and Intellectual Property

Section 46. The Institute gives precedence in the intellectual property. Therefore, the permitted or copyright software of the Institute has, the user could ask for it as necessary. And the Institute prohibits to allow the user to install or use any illegal software. If it has been found to infringe the copyright, the Institute has judged that the fault is individual fault for the user only.

Section 47. The provided software is assumed that it is necessary for work. Prohibit any user install, remove, change, correct or copy to use the other place.

Preventing Malware

Section 48. The user's computer must be installed the antivirus program as the Institute declared. Except for those computers are computers for education, development, protection system which are allowed by the Digital System Division.

Section 49. Data, files, software or anything that the user has got from the other user must be checked computer virus and malware program before using or record every time.

Section 50. The user has to update the data for checking and update patch for damage protection.

Section 51. The user has to be careful of the virus and malware program all the time, including the user has to inform the administrator when has found the unusual thing.

Section 52. Whenever the user has found that the computer is infected by a virus, the user would not connect the computer with the network and has to inform the administrator.

Section 53. Prohibit to hidden copy, change, remove of data, message, document or any matter that belong to the Institute or others without permission from the authorized person.

Section 54. Prohibit to distribute the computer virus, malware program or any dangerous program that may cause the damage to the Institute asset.

Law and Compliance

Section 55. Any law declared in Thailand and the Institute regulations are the importance, which the user must be aware and perform strictly, and do not break those laws. The fault is assumed to be individual fault that the user has to be responsible for it.

Part 2

Physical and Environment Security

Section 56. Building, places and information system working areas mean the place located the computer system, network system or other information system, the provided areas for computers and accessory, working areas for the computer officers, including personnel computer installed on the desk.

Section 57. The computer room must be as the following;

(1) Define to be strictly restricted area or restricted area only as to the consideration of the priority situation;

(2) It must not located in the areas that many people pass;

(3) It must have not notice board or notation to inform the important system inside that place;

(4) It has been locked or put key at the window, door or room regularly when there is no officer;

(5) If necessary, the copy machine or facsimile machine have been separated from such areas;

(6) Do not permit to take a photograph or record video tape in such areas strictly;

(7) The areas are provided for transfer of the goods separated from information asset in order to prevent the system from the unpermitted person.

Section 58. The physical security of the system, for the benefit of the security equipment at services system location should install the modern and appropriate technology.

Section 59. The Institute assigned officer or permitted person only are qualified to enter strictly restricted area or restricted area only.

Section 60. There should be the security for mobile computer and accessory when they are used, borrowed/returned, or others according to the Institute's regulations on Information Security management.

Section 61. Electricity system and ventilation system must be safe and appropriate. The backup electricity is provided when the electricity disorders. And the backup ventilation system is provided to control the room temperature and moisture steadily.

Section 62. Electrical wire and cable system is secured by electric or cable wiring through the special channel where normal person could not enter easily.

Section 63. Mitigation for fire protection and natural disaster provided by installing the fire equipment for computer system, natural disaster prevention equipment that are available to use. The places, materials are necessary for rehabilitate the system and safety data backup areas.

(1) Fire protection, the areas are installed the firefighting system especially for stop the fire immediately and effectively without any damage to electricity equipment, electronic equipment or computer.

(2) Media storage, magnetic media or other media for data backup and storage, must be kept safe and effective.

(3) To destroy the unwanted things, magnetic media or recorded media to prevent not to return to be used means to overwrite, degauss or destruct.

Section 64. There must be emergency plan and policy such as IT Contingency Plan, Database and information Risk Management Plan, Movement Plan, Emergency Information System Destruction Plan and Information System Security Policy.

Section 65. Provide security guard and information system protection, and set up the meeting to clarify the steps of investigation and proof and obstruction in the area regularly and strictly.

Part 3

Access control Policy

Information Access Control

Section 66. The Institute sets out the security mitigation for control of access of office information system. The outsider wants to access the information must be permitted from the Department of Digital Development or assigned officer.

Section 67. System administrator must define to access data and data system properly, and the officer's responsibility before using the information system, including reviewing regularly.

Section 68. System administrator should install data entry and follow up office information system for finding infringe.

Section 69. System administrator must provide data entry in detail, pass of the system location of both permitted person and unpermitted person for audit evidence.

Information System Access Management

Section 70. System administrator must provide for registration of new officer of the Institute. It should appropriate steps officially for rights to access as necessary. It includes the steps for cancelling in case resign or change the position.

Section 71. System administrator must define the important information technology system such as application program, e-mail, wireless LAN, internet system, etc. They must be permitted the right on duty with the written permission of superior, and reviewing such right regularly.

Section 72. System administrator must manage the right to access the system and password for the following officers;

(1) Define the change and cancelling when the officer has resigned from the position or cancelling the access;

(2) Hand on temporary password to the user, should avoid to let other send e mail by using unprotected password;

(3) Should let the user confirm the password when received it;

(4) Should let the user not record or keep password in computer system in the unprotected access form.

(5) The user and password should not repeated.

(6) In case of necessary, the highest right has to permit to the highest right user, such user must be approved by superior. The time limit of access and at once suspension when resign from the position including level of access are defined. The password has been defined different to regular user.

Section 73. System administrator must design and manage the levels of confidential to access the data directly as the levels of confidential, and access to system including the destruction of the data of each level of confidential as the following;

(1) It must control to access each level of the data directly or through system;

(2) Defining the username and password for authentication in each level of data;

(3) It should limit the time and suspend at once when the time is out;

(4) Transmission of important data through public network system should encrypt in standard such as SSL, VPN, or XML encryption and so on;

(5) The password is limited the time period according to the importance of the level of the data;

(6) Mitigation for data security is defined in case of the computer is used outside the office such as repairing, the backup and removing of the data should be done before.

Part 4

Network and Server Policy

Section 74. The Institute has set out the measures to control the entry of the server room.

Section 75. The user brings the computer or accessory connecting with the office computer or network system, he should be permitted from the Governor or assigned officer, and perform regarding to this policy strictly.

Section 76. The permission to use web server and sub domain name is done from the Governor or assigned officer by written document. And the user must not setup any program impacting to system and other user.

Section 77. Prohibit to install any additional equipment into central system such as router, switch and so on without the permission of the system administrator.

Section 78. System administrator must control to access network system effectively as the following;

(1) The right must be limited for the user be able to access network system for permitted users only;

(2) The route should be limited for access the network system together;

(3) The route from the computer network to the server is limited for the user could not use the other route;

(4) All office network system connecting to the outside network system should pass through the threat protection equipment, including be able to detect the malware program;

(5) Intrusion prevention system/intrusion detection system should be installed in the network system for checking the unusual user access the office network system;

(6) Access of the network in the office through internet system must be login and authenticated for integrity.

(7) IP address in the office should be prevented from the outsider to know;

(8) Network diagram is provided in detail of scope of internet system and intranet system and other accessory including update regularly;

(9) The use of any equipment to check the network system must be permitted from the system administrator and be limited as necessary.

Section 79. System administrator must control and be responsible for server to improve or change any values in systems software.

Section 80. The Institute must collect the computer traffic data or Log data for integrity and identity as the following;

(1) Log data should collect in the real time, complete and correct data and define the level of confidential. And system administrator could change the data except the IT auditor or assigned officer;

(2) The record of access, application logs, details of threat prevention system are done such as pass system record, command line and firewall log and so on for checking benefit. The records must be kept at least 90 days after using the service;

(3) The inspection of the user record must be performed regularly;

(4) The record protection to be altered, changed must be by special officer only.

Section 81. The Institute has defined the mitigation for control of the network system and server for securing the system from outside as the following guidelines;

(1) The user from the outside office need to access the office network system and server must be permitted from the Governor of the Institute using written document;

(2) Control of port into the system must be restricted;

(3) Any means for access the data or data system from remote must be approved by the Governor of the Institute;

(4) Access system from remote, user must declare evidence with the reason or necessity to carry out with the office sufficiently;

(5) Access the system must be authenticated from the office system.

Part 5

Wireless Policy

Section 82. The system administrator must control the leakage signal of access port to the surrounding areas the least.

Section 83. The system administrator should change the value of the service set identifier or SSID as set as the default at once after receiving the access port to use.

Section 84. The system administrator must set up the value of wired equivalent privacy, WEP or Wi-Fi protected access, WPA in the data password between wireless LAN client and the equipment of access port and should define undeclared value in the wireless system.

Section 85. The system administrator should the method to select to control MAC address (Media Access Control Address) and username, password as defined only for the integrity of the access wireless system.

Section 86. The system administrator should install firewall between the wireless system and office intranet system.

Section 87. The system administrator should permit the wireless system user to connect only with the VPN (virtual private network) to prevent the outside threats into wireless system.

Section 88. The system administrator should use the software or hardware to inspect the wireless system security and record the inquiry evidence and report every 3 months. If it is found that there are some unusual in wireless system, the system administrator reports to the Governor of the Institute at once.

Section 89. The system administrator must control the outsider to access the wireless system through the intranet system and other database of the office.

Part 6

Firewall Policy

Section 90. The Institute by the Digital System Division is responsible for manage, install and define all values of firewall.

Section 91. The definition of basic data of all network must be refused.

Section 92. All route connecting to the internet unpermitted by the policy must be blocked by firewall.

Section 93. The internet user must log in the account every time to access.

Section 94. All the changes in firewall such as parameter values, services values and permitted connection must be recorded every time of changes.

Section 95. Access to firewall equipment could be done by the assigned person only.

Section 96. The computer traffic data must be recorded not at least 90 days.

Section 97. The policy to service the internet to the client computer would open port connecting to the basic general program that the Institute has permitted. If necessary, the other port would be used to connect, the permission is done by the Governor of the Institute.

Section 98. The network computer would define the permitted value for service the special port as necessary to the real service network computer.

Section 99. The values of firewall would be changed and backup every 3 months and be recorded every time of change.

Section 100. Network computer must not be permitted to connect to the internet except for the necessary only.

Section 101. The Institute has the right to suspend the client illegally or risk program for security until resolving.

Section 102. The remote login from outside into the network computer or internal network would be permitted from the Institute.

Section 103. The person who break the firewall policy would be suspend to access the internet at once.

Part 7

E-mail Policy

Section 104. The registration of using e-mail must complete the form to use e-mail in the Institute and submit to the officer.

Section 105. The first receive of password in e-mail, and when login first, the password should be changed at once.

Section 106. It should not keep or record the password in computer system.

Section 107. The password should be changed every 3 months.

Section 108. The other e-mail address should be used for read or send except having the permission. The owner of the e-mail address is responsible for access the e-mail.

Section 109. After using the e-mail system, the user has to logout every time.

Section 110. Sending the confidential data through e-mail should not declare the importance or confidential message in the title of e-mail, except using the code that the organization defined and be careful to declare the e-mail address of receiver correctly to prevent sending mistake.

Section 111. Do not send spam mail.

Section 112. Do not chain letter.

Section 113. Do not e-mail illegally or breaking other right.

Section 114. Do not send virus infected mail to others intentionally.

Section 115. Define the name of sender every mail.

Section 116. As necessary, e-mail data are backup regularly (though the Institute has backup the data, but for a limit of time, therefore, the very old used e-mail should be backup by himself).

Part 8

Internet Security Policy

Section 117. Do not use office internet system for commercial purposes individually. And do not access into website improperly such as immoral website, impact to security of the country, religion, king or antisocial website or violate the personnel copyright or data that damage the office.

Section 118. Do not reveal office confidential data which is not declared officially through internet system.

Section 119. Be careful to download program through the internet system. The download and update program would not violate any copyright.

Section 120. In using electronic board, the important data of the office would not be revealed.

Section 121. In using electronic board, do not use the abused or aggressive words to damage the office reputation or public relation.

Section 122. After using the internet, close the web browser for protection from other user.

Part 9

Intrusion Detection and Prevention System Policy: IDS/IPS Policy

Section 123. IDS/IPS policy is the policy to install the inspection system for threats and security of the network. The office asset and information system and network system are secured and are procedural guidelines for inspection of threats and the role and responsibility.

Section 124. IDS/IPS policy cover all hosts in Institute's network and data network including all data routes that may not be in the internet network.

Section 125. All system that could access in the internet or public must be inspected by IDS/IPS system.

Section 126. All hosts and networks transmit into the IDS/IPS must be audited in the inspection result.

Section 127. Update Patch/Signature of IDS/IPS is inspected regularly.

Section 128. Inspection of event, traffic data, user behavior, activities and record of data entry into network regularly every day by system administrator.

Section 129. IDS/IPS work under basic control rules of firewall used to access the network of normal information system.

Section 130. Sever installing host-based IDS must be inspected the data every day.

Section 131. Behavior of the user, activities or all events which risk to the threats, attach to the system, inquiry or attempt into the system successfully or not must report to the superior at once.

Section 132. Behavior or inquiry or system unusually must be informed the superior within 1 hour.

Section 133. All the inspection record must be kept for at least 90 days.

Section 134. The form of responding are reports of inspection, steps for procedures to reduce the damage, delete malware software, protection the foreseeable event and perform as regarding to the plan.

Section 135. The Institute has the right to stop the connection of the network that is risk to the system without informed.

Section 136. The section to whom that try to infringe the Institute policy or illegal access into the system, attach the system or risk behavior to information system would be suspended at once. If such behavior violate the Computer-related Crime Act B.E 2550 (2007) or the fault that damage to the data or asset of the Institute would be legal action.

Part 10

Backup Policy

Section 137. Copy of data and software is provided and prioritized from the most to the least as necessary of information system backup.

Section 138. The integrity of the data backup and retrieved data both in software system and information system. The steps to be performed are separated for each information system.

Section 139. Keep the data in data media, and type the name of data with software system, date, backup time and responsible person concisely. The backup data would be kept in another place that must be tested the backup media regularly.

Section 140. The emergency plan is provided the data retrieved within appropriate time.

Part 11

Database Security Policy

Section 141. This policy aims to prevent from the access, change, transfer the data by irrelevant user, including providing backup system and restoring the data.

Section 142. All types of data and information in database are prioritized to protect the eligible person, including necessary detail for security mitigation section 3, the secret data could be performed according to the Rule on Maintenance of Official Secrets, B.E. 2544 (2001).

Section 143. The agency owns the database, user right and authorized in task line are person who consider the qualification of user and the program permitted to use those data, and provide log file for database access, for integrity of data.

Section 144. In case, the database are used among the agencies, the Memorandum of Understanding is provided.

CHAPTER 3

Performance in Case of Violation of Security

Section 145. Objectives. For being the procedure guideline when violate the information security of the Institute. And to reduce the damage that may happen from the attack or avoid to be at least. Including, inspect the cause of damage for improving protection measures repeated, and define the procedure to person whom violate security.

Section 146. The procedure when the security is violated;

(1) When it is found or suspect to violate information security system or unusual in information system, inform or report to superior or officer of information security system rapidly;

(2) Officer of information security system performs as the following;

(3) Report initially to the Director of Digital System Division when it is found the violation of confidential information;

(4) Reduce the damage initially by settling, cancelling suspected information system. If the information is confidential, cancelling would be performed at once, and inform the owner of the confidential information.

(5) Survey the damage from the violation, causes, and weakness of information and communication.

(6) Report the incident to the Director of Digital System Division of the Institute, including the protection guideline to prevent the situation repeated.

(7) In case the loss of the secret code system used in information system or suspect that unauthorized person know the secret code system, cancel or change the secret code system at once. Then report to the Director of Digital System Division of the Institute at once.

Section 147. Responsibility of the Director of Digital System Division of the Institute;

(1) Inform the agency owning the information rapidly;

(2) Set up the committee to investigate and find responsible person and offender rapidly;

(3) Inform the original agency penalize responsible person and offender according to the damage value to the information system or as the law.

(4) Command to improve the weakness and protect to occur repeated.

Section 148. To carry out the information security measures completely and rapidly, the terminology is address in the attached notification, including computer words with similar meaning as in the attached notification.

It is to be informed and performed.

Given dated 29th March B.E.2560

(Mrs. Luxsamee Plangsangmas)

Governor

Digital and Information Office

List of terminology

Officer for securing information security of the office

1. "System Administrator" means a person who at least has the knowledge of hardware, software of the system and be appointed to perform as the following;

(1) Execute and secure computer equipment which is the server to services to other agencies.

(2) Control and inspect system operation;

(3) Inspect, control, secure and maintain the system;

(4) Security of the system such as confidential, maintain and readiness.

2. "Database Manager" means a person who at least has the knowledge of database computer system management and be appointed to perform as the following;

(1) Control and secure database such as collection, addition, change, delete, structure setting, use, storage and retrieval;

(2) Select, extract and define types of data to storage in the file;

(3) Protect the security of the database such as secret, existing and readiness of the database;

(4) Inspect database and analysis data;

(5) Control and services to use database;

3. "Network Administrator" means a person who at least has the knowledge of hardware, data communication and equipment in the network system and be appointed to perform as the following;

(1) Define IP Address for office computer network by coordinating with government or computer network system service officer of the Institute;

(2) Define the account and password of user in network;

(3) Take care of computer network within the government;

(4) Take care of infrastructure and network system equipment such as modem telephone, hub etc.

(5) Secure network system such as secret, , existing and readiness of the database.

4. "Programmer" means a person who at least has the knowledge of computer system, computer and database programming, and be appointed to perform as the following;

(1) Programming and develop as assigned;

(2) Provide the data to test program;

(3) Maintain developed program;

(4) Secure the program such as secret, existing and readiness of the database;

5. "Information System Workspaces" means the areas installed the computer system, network system or other information system or preparing the data, storage of the computer equipment, areas for the computer personal, including personal computer on the desk.

6. "Information System Network" means communication or transmission of the data among information system of the Institute such as intranet system, internet system etc.

7. "Classified information" means the information in the form of data or message recorded and prioritized and limited to access, including floppy disk, secret code, code and password and material or document.

8. "security incident" means case declares the incident, situation of services or network possibility to happen, obstruct the security policy of protection measure failure or unforeseeable incident relating to the security.

9. "Unpredictable security situation" means situation that has not been expected to happen. It may the organization system intrude or attack and threat to the security.

10. "Threat" means danger to information system by person, thing or event intentionally or not intentionally. It causes the data of the information system revealed, changed, distort, damage, disorder or any performance as the threat desired.

11. "Vulnerability" means weakness or fault of the information system in the proper type. It could be used to harm the information system. The same threat may not be the same risk in each workspaces. The risk is used as for decision of the preparation of the density of the security system.

12. "Account" means symbol or set of letters in the unique differently for identification of account owner or groups of persons who access the system. The account is the tool to protect the security with the password.

13. "Log file" means all record of the procedure of relating data processing equipment or run the operation priority from start up until finish the task. It includes activities for inspection of integrity later , to elevate the standard of technology and information system security of the Institute to be international. The Institute has approved policy of information system security by set out the guideline of framework and plan. And the Institute implements the policy of information system security completely. Therefore, all police and officer under the Institute have to be informed and perform according to the guideline of the policy of information system security.

14. "Malware" means program of command set resulting that computer or computer system or other command set damaged, destroyed, changed of added, disorder or operation in different from the command.

15. "e-mail" means system that a person used to transmit the message together through computer and network. The data transmitted are letters, photographs, graphics, animation and sound. Transmitter could send the news information to one or many receivers. the standard for data transmission are such as SMTP, POP3 and IMAP and so on.