Lao People's Democratic Republic
Peace Independence Democracy Unity Prosperity

Ministry of Posts and Telecommunications No. 3623/MoPT
Vientiane Capital, Date 11th December 2011

Instruction
on Computer Safety

- Pursuant to Law No. 61/NA, dated 15th July 2015 on the Prevention and Defense of Cybercrime.
- Pursuant to Prime Ministerial Decree No. 22/PM, dated 16th January 2017 on the Organizational Structure and Activity of the Ministry of Posts and Telecommunications.

Minister issues instruction as follows:

I. Objectives.

This instruction is aimed to roll out the content in article 24 of the Law on the Prevention and Defense of Cybercrime that relating to the specific measures on governing computer safety in order for the creation, prevention, management, surveillance and monitor on computer safety are united throughout the country.

II. Network creation and prevention.

1. Network creation

The creation of a safe computer network to use in management, administrative, services, and the use of Information Technology and Internet, network management authorities should follow:

1.1. Creating network diagram for convenient management, installation, setting, and repairing;

1.2. Creating specific sectors for computer network according to their functions such as internal and external computer network making it available to systematical monitoring threat;

1.3. Validating devices to be installed in computer network and main computer network for instance scanning virus on computer and determining technical setting in those devices;

1.4. Installing programs to monitor work status of those devices being connected to computer network;

1.5. Accession to organizational computer network through internet connection must be recorded for each time of login and must be correctly authenticated;

1.6. Movement and additional installation of devices are prohibited such as network connection device, computer connection device, main computer network system device or any other devices without permission from system management authorities.

2. Main network system protection

To ensure a quick and accurate information providing system from the main computer network system, the management authorities of the main computer network system should follow:

2.1. Determine an inclusive safety policy, accessible or preventing information circulation that might affect the system of main computer network;

2.2. Ability to record all the changes happened to main computer network system for 24/7 or every time that changes happen to the setting of the main computer network system;

2.3. Having procedures and methodology to monitor the safety system of the main computer network, if found any abnormal or having found any changes, a prompt solution must be addressed;

2.4. Recording the history of mal-operation that happens to main computer network system as well as the operation of users, login-out to/from the system;

2.5. Designate particular personnel responsible for the main computer network system to set up, solve, change, and to run the network system responsively;

2.6. Determine necessary service route for accession, use, improvement, setting, solving, and adjusting the network system in order to reduce the risk of being disrupted of the main network system;

2.7. External accession to the main computer network system (remote log in) or accession to internal network devices via FTP, FTPS, SSH must be coherent with organization's policies.

3. Wire network protection

To assure a safe computer network being connected to main computer network system, computer network and the main computer network system managers should follow:

3.1. Install and use devices with international standards;

3.2. Install intrusion prevention system to monitor the intrusion of computer network and find ways to keep computer network secured;

3.3. Install attack prevention system DDoS that includes intrusion search and intrusion elimination system to prevent the main computer network system and computer network from stop working;

3.4. Install Firewall to screen intrusion between internal and external computer network and to set up the system to record information circulation, log in-out of computer network in log management in order to examine, analyze intrusion, and plan for prevention;

3.5. Accessing computer network from outside must be approved from system management authorities and be strictly controlled such as authentication and rights of users;

3.6. Every time of the examination on operation of computer network needs to get approval from system management authorities or head of organizations;

3.7. Edition or changes wish to be made on devices in computer network, computer network management authorities must have their technical staff informed and followed instruction;

3.8. Having timeframe for monitoring, verification, and restoration. Adjustment computer network must be carried out from three to six months per time yearly.

4. Wireless network protection

To assure computer network being connected to the main computer network system through the use of wireless computer to execute main computer network management system should follow:

4.1. Install and use devices that have international standards;

4.2. Set password for the log-in to manage signal from wireless fidelity router (Wi-Fi) and authentication password;

4.3. Install Wi-Fi at a proper position and determine the areas of the use at a convenient and easy for restore place;

4.4. Users are not allowed to bring wireless devices to install or use in their organizations such as Access point, Wireless Router, and Wireless card;

4.5. Determine computer password (MAC address) that enables the use of Wi-Fi for authorized computers or authorized list with password that are set within organization;

4.6. Change the name of Wi-Fi that is set from manufacturer to the name of the organization (Service Set Identifier);

4.7. Set a proper Wi-Fi devices based on safety standard setting list for devices;

4.8. Set up wireless router to protect accession to wireless protected access 2 by using password;

4.9. Determine regulations for the use of organization's Wi-Fi

4.10. Having hardware or software in place to verify the safety of Wi-Fi and to record the abnormal uses

4.11. Any abnormal use of Wi-Fi found should be reported to the management authority for prompt solutions.

5. Malware prevention

In the prevention of Malware or computer virus from not spreading to shared computer networks, computer management authorities and users should follow:

5.1. Install anti virus programs on computers with permission to use (software license) and restore them in a working mode;

5.2. Use Windows Firewalls that come with window operation system to prevent virus from intrusion;

5.3. Use virus detection or anti-virus programs that come with operation system such as Windows Defender;

5.4. Detect and remove computer virus in information files and other documents before using and saving information files on files storing devices;

5.5. Detect and remove computer virus on external hard disk, memory stick, and others before using;

5.6. Never click on links or open documents that do not have sources or the attached documents in electronic mails that do not include senders' addresses;

5.7. Never open website or download computer programs that do not have trusted sources;

5.8. In an event of virus, instant virus removing must be applied or informing the case to concerned authorities.

III. Network management

1. Computer user listing

Computer management authorities should determine rights, scope, and users' history that will help enable verification and monitoring the use of computer network as follows:

1.1. Accession to computer network;

1.2. Accession to importation information in document management system;

1.3. The use of specific programs such as accounting, human resource management, computer database, and others;

1.4. Should immediately stop or remove irrelevant computer network users' accounts in organizations;

1.5. The irrelevant users are not allowed to make copies, destroy or change organizations' information.

2. Computer password setup

Computer network management authorities or its owners should set password for accession to computer as follows:

2.1. Password should include digits, uppercase and lowercase letters and symbol or marks;

2.2. Password should contain more than 8 letters;

2.3. Easily doubtable password should be avoided such as abcdef, aaaaa, 123456;

2.4. Password that contains users' personal information such as name, surname, date of birth and phone number;

2.5. Shall not allow other people to use one's own user name and password;

2.6. Shall not determine password in dictionary;

2.7. System management authorities should change password 03 months per time;

2.8. General users should change their password 06 months per time.

3. The use of electronic mail

The use electronic mail in a correct and safe way should follow:

3.1. Use electronic mail that is created and managed by one's own organization;

3.2. Immediately renew password after first log-in;

3.3. Renew password for electronic mail should follow the process in above section III, number 2;

3.4. Set up password for confidential information before sending through electronic mails;

3.5. Shall not save password in computer or in places that can be easily seen;

3.6. Shall not use others' electronic mails without permission;

3.7. Shall not fake senders' names by hiding one's own address or source of electronic mails;

3.8. Shall not use organization's electronic mails to register for services in websites;

3.9. Shall logout from electronic mail system every time after finished using it.

4. The use of internet

To use a secured internet, computer network management authorities and users shall follow:

4.1. Determine regulations for the use of internet in organizations so that It can be conveniently checked and monitored;

4.2. Computer network management authorities shall determine internet connection routes through Firewall system for their users in organizations;

4.3. Computer network management authorities shall determine the rights to access to information based on specified organizations' responsibilities;

4.4. Internet users shall validate information retrieved from internet before utilizing it;

4.5. In an event of accession to database through website browsers, internet users shall immediately close web browsers to prevent intrusion in database;

4.6. Entering information password every time before sending through internet network.

5. Safety awareness

Organizations or safety management units shall organize activities that will help raise awareness among internet network users in organizations so that they could acknowledge about internet intrusion as follows:

5.1. Organizations or safety management units shall regularly organize trainings to help maintain computer network for users and management authorities within organization. Being prepared for harm that might happen in order to be able to restore damaged computer system back to working mode;

5.2. Create motto on computer intrusion for instance advertisement, magazines, videos, safety tips to disseminate within organizations;

5.3. Shall not press or express any extreme behavior when computers or programs stop working;

5.4. Shall not fix or solve problems happened to computer system in organization without permission;

5.5. In an event of not knowing how to fix problems happened to one's own or organizations' computers, computer system management authorities shall be informed;

5.6. Read the popped up warning messages from operation system before accepting;

5.7. Immediately log out from service system when not using it;

5.8. Lock computer screen when not using it;

5.9. Study and follow a guideline to use computer network devices safely.

6. Computer data restoration

To assure the safety of computer data, the prevention of damages, and the regular function of computer, computer network management authorities and the users shall follow:

6.1. Determine process or methodology to store data for instance backed up data, type of data, amount of backed up data, data storing process, the store of data, determination of time to store data, places for data to be stored and the recording of operation history;

6.2. Create a safe data storing system;

6.3. Store data in external hard disk regularly;

6.4. Validate the stored data from 03 to 06 months to assure accuracy and readiness of data;

6.5. Regulate plans or methodologies to regularly recover data capacities immediately when system downs/collapses.

IV. The store of safe data.

1. Physical safety

Physical safety shall follow:

1.1. Names, date and time on the coming in-out of people at data center shall be recorded;

1.2. The entry and exit to/from equipment room must be installed fingerprint screening system, required for password to enter and exit the specified doors, requested for identification cards and installed closed-circuit camera for monitoring and the safety;

1.3. Strictly create policies or regulations to service customers;

1.4. Set up special technical room for service users to be able to inspect, monitor and for the convenience of improving equipment system of their own;

1.5. Install warning alarm to notify when emergencies happen;

1.6. Shall have automatic uninterruptible power supply system to respond to when electricity does not function properly;

1.7. Temperature inside equipment room should not exceed 20-22 degrees Celsius;

1.8. Shall install smoke or heat smoke detection system to notify the circumstances happening inside the buildings;

1.9. Regularly test on harm prevention systems in data center in order for their readiness to function.

2. hard ware maintenance

In order to keep computer network safe, rightly maintenance of hard wares, validation of operation or function shall be conducted as follows:

2.1. Budgeting for the purchase of hard wares;

2.2. Users or computer network management authorities must regularly check hard wares to be used in computer network management of their own, if damages or expired date found immediate replacement shall be planned;

2.3. Computer system, main network system, connecting devices and receiving/forwarding signal devices must contain uninterruptible power supply (UPS) to ensure the continuous function when confronting irregular electricity supply;

2.4. Routinely cleanse up computers to keep dust away from screen, keyboard, mouse, and computer case.

3. Software maintenance

To maintain a safe computer network, software maintenance, operation monitoring or accurate function shall be practiced as follows:

3.1. Regularly repair the computer operation system;

3.2. Install and use authorized software license alongside with monitoring and inspecting valid date;

3.3. Disk defragment to increase the data running capacity;

3.4. Remove the unused computer programs.

4. Electronic data safety

The store of a safe electronic data shall be prioritized in order:

4.1. Prioritize the importance of electronic data;

4.2. Use password to access electronic data;

4.3. Determine rights for accessing electronic data;

4.4. Electronic data stored in different places must be accurate and consistent in terms of quantity and content;

4.5. Use software and destruction machine to eliminate data saved in devices such as hard disk, CD, DVD, hard drive.

V. Coordination and Cooperation

Solving emergency problems happened to computer in data center shall be acted as follows:

1. Data center shall establish a computer safety unit to coordinate for the defense and emergency solving work (Lao CERT center);

2. Apply the process, technical standards when solving emergency problems happened to computers;

3. Create and notify address, phone number and email to relevant organizations or computer emergency defense units;

4. Coordinate to organize technical trainings, practicing to solve and respond to computer emergencies.

VI. Safety monitoring of main computer network and computer network system

1. Cybercrime monitoring.

1.1. Computer network management authorities and its general users shall follow information, warning and ways to handle with website hacking threat, computer network intrusion, and the expansion of Malware and others;

1.2. Follow prevention guidelines and apply technical solutions from safety management units or from the defense and computer emergency solving center that issue notification periodically.

2. Risk assessment.

To prevent the system of main computer network and computer network from damages, system management authorities shall have risk assessment in place and follow these steps:

2.1. Analyst the intrusion on computer network that might happen;

2.2. Assess the risk of connecting devices of computer network;

2.3. Assess the risk of operators that might occur from operation, prioritization of information accession or information accession services;

2.4. Assess the technical risk that might happen to computer, tools and equipment from being attacked by virus, computer programs or the computer system hacking;

2.5. The risk that might come from natural disasters that will cause damages such as impaired function of the main computer network and computer network.

2.6. Impact assessment and damages to organizations.

3. Safety monitoring

Checking for defects or gaps that might occur to the main computer network that requires the system management authorities to follow these steps:

3.1. Check the gaps in main computer network system and computer network to seek for defects, ways to improve, prevent, and solve;

3.2. Test the operation of the main computer network system and computer network inside outside organization through hacking or stopping the operation.

4. Safety surveillance

Data center safety surveillance shall follow these steps:

4.1. Install surveillance system to monitor and check the intrusion that might happen to main computer network system and computer network;

4.2. Establish monitoring surveillance to check the intrusion on the main computer network system and computer network for 24/7.

VII. Implementation

Defense and computer emergency response unit is assigned to collaborate with relevant sectors including local administration to advertise, disseminate, guide and implement this Instruction for its effectiveness.

Ministries, organizations equivalent to ministries and local administration, individuals, legal entities residing in Lao PDR shall accurately acknowledge and practice.

VIII. Effectiveness

This Instruction is effective since the date of signature and practicable 15 days after posting on Lao Official Gazette.

Minister

(Signature and Sealed)

Dr. Thansamay kommasith