Lao People's Democratic Republic
Peace Independence Democracy Unity Prosperity

National Assembly ` No. 61/NA
Vientiane Capital, 15 July 2015

Law
On Resistance and Prevention of Cybercrime
Part I
General Provision

Article 1 Objectives

This Law determines the principles, regulations and measures regarding the management, monitoring of cybercrime resistance and prevention activities in order to enable the effectiveness of such activities with the aim to resist, prevent, restrain and eliminate the crime, to protect database system, server system, computer data and to guarantee the security of the nation, the peace and orderliness of the society, the ability to link with regional and international network, and to contribute in the protection and development of the national socio-economic in a progressive and sustainable manner.

Article 2 Cybercrime Resistance and Prevention

Cybercrime is a wrongful act in the computer system that cause the loss to the state, individuals, legal entities, organizations and society based on the behavior specified in Article 8 of this Law.

Cybercrime resistance and prevention is an activity to restrain, eliminate, suppression of individuals, legal entities and organizations that have direct rights and duties in finding out and implementing the cybercrime resistance and prevention activities as specified in Article 19 and 24 of this law.

Article 3 Definition of Terms

The terms applied in this Law shall have the meaning as follows:

1. **Crime** refers to wrong doing as stipulated in the Law on Criminal Procedures and other laws that determine criminal punishment;
2. **Computer system** refers to an electronic equipment or a set of computer equipment that link together the operational system through determination of orders, set of orders or other things in order to enable the electronic equipment or sets of computer equipment to perform data processing automatically in one or many computers that are connected to each other through the computer network and internet networks;
3. **Server System** refers to the service system through computer system, which consists of Database Server, Web Server, Mail Server, File Server and others;
4. **Computer Data** refers to any data, messages, programs or database system, personal data, computerized traffic data in the form that can be processed and enable the operation of the computerized system;
5. **Database System** refers to data being saved in electronic file that can be manageable, improvable and usable;
6. **Personal Data** refers to data related to or referred directly to the character or ……., activity of individuals, legal entities or organizations in a direct or indirect way;

7. **Data Traffic through Computerized System** refers to computer data relating to the communication through computerized system which being created by the computer system that is a part of the communication chain which indicate the sender, starting point, mediums, road, destination, date, time, size, duration of communication, type of services and others that are related to the communication through such computerized system.

8. **Service Provider** refers to a person who provide a service in the field of communicating the information through the computerized system and/or computer data maintenance service provider;

9. **Data Processing in Automatic Form** refers to the process of data calculation and processing in the computerized system through the computer program;

10. **Program** refers to a system or set of commands that the computerized system can operate in order to ensure the result as provided;

11. **Virus** refers to a special program being created which can be expanded, cause damages and destroy the computerized system, computer network and computer data.

12. **Malicious Code** refers to a set of computer command created in order to destroy the computerized system or to steal the computer data;

13. **Phishing** refers to any newly created website that is similar to the former one in order to deceive data from the users;

14. **Vulnerability** refers to defect of the incomplete and unimproved program or software causing malicious person can make use in order to destroy the system, steal data, change data, etc.,

15. **User Data** refers to any data sending to the user, such as postal address, electronic address, geographical address, Internet code number, telephone no. or others that being used in the computerized system;

16. **Special Protection Measures** refers to the use of apparatus and/or special computer software in order to resist and prevent the user's access to the computerized system;

17. **Online Social Media** Refers to the communication through the internet network system in order to disseminate the information to the public through the use of computer assembly material and other communication object;

18. **Moving Picture** refers to a build-up picture that can be moved as actuality through the electronic apparatus such as Cartoon Film.

Article 4 Government Policy on Cybercrime Resistance and Prevention Activities

The state encourages the computerized system to be used in a safe, convenient, quick and fair manner as well as to protect the legitimate rights and interests of service provider, service users of computerized system and computer data in accordance with the laws and regulations.

The state sets condition and facilitates the implementation of the cybercrime resistance and prevention activities through the provision of budget, builds and recruits personnel, vehicles, equipment, study and apply modern technology, build infrastructure to enable the effectiveness of such activities.

The state considers cybercrime resistance and prevention as main activities and problem solving as significant tasks.

The state encourages and promotes individuals, legal entities and organizations (both domestic and foreign) to invest in the production in terms of technique and technology as well as to participate in cybercrime resistance and prevention activities.

Article 5 Principles on Cybercrime Resistance and Prevention

In the cybercrime resistance and prevention activities, the following principles must be followed:

1. The conformity with the policy, laws, strategic plan, the national socio-economic development plan;
2. The security of the nation, the peace, orderliness of the society, culture and fine tradition of the nation;
3. Safeguarding the confidentiality of the nation, official, individuals, legal entities and organizations;
4. The uniformity, safety, convenience, quickness and fairness;
5. The protection of legitimate rights and interests of service providers, computerized system service users, computer data in accordance with the laws and regulations;
6. The social participation;
7. The implementation of international convention and treaties in which Lao PDR is a partner.

Article 6 Scope of Law Application

This law is applied for individuals, legal entities and organizations (both domestic and foreign) who live, perform activity, and study on the use of computerized system and computer data in the Lao PDR.

Article 7 International Cooperation

The states open up and promotes cooperation with foreign countries, regional and international levels with regard to the cybercrime resistance and prevention activities through the exchange of lessons, experiences, information-technology, upgrading of professional level, knowledge and capacity building of staff, data verification and data proof in conformity with the laws, regulations of the Lao PDR, with the international convention and treaty in which the Lao PDR is a partner.

Part II
Cybercrime-Prone Behaviour

Article 8 Cybercrime-Prone Behaviour

The cybercrime-prone behaviour includes:
1. Disclosure of safeguarding measures for accessing computerized system;
2. Unauthorized accessibility to computerized system;
3. Censoring of content, photos, moving pictures, sound and video without authorization;
4. Stealing data in the computerized system without authorization;
5. Causing the losses through online social media;
6. Dissemination of pornography through computerized system;
7. Interference of computerized system;
8. Forgery of computer data;
9. Destruction of computer data;
10. Business operation related to computerized system cybercrime tools.

Article 9 Disclosure of Safeguarding Measures for Accessing Computerized System

Disclosure of safeguarding measures for accessing computerized system is to bring special safeguarding measures for disclosure without authorization which causes damage to the state, individuals, legal entities, organizations and society.

Article 10 Unauthorized Accessibility to Computerized System

The unauthorized accessibility to computerized system is the use of electronic apparatus in the computerized system with special safeguarding measures or to steal commercial, financial data, confidentiality and other data of individuals, legal entities and organizations.

Article 11 Censoring of Content, Photos, Moving Pictures, Sound and Video without Authorization

Censoring of content, photos, moving pictures, sound and video without authorization is to re-build, add or adapt from the original version through the electronic method or other methods in order to disseminate through the computerized system which cause the loss to individuals, legal entities and organizations concerned.

Article 12 Stealing Data in the Computerized System without Authorization

Stealing data in the computerized system without authorization is to catch up data being received or transferred through the computerized system by using electronic apparatus.

Article 13 Causing the Loss Through Online Social Media

Causing the loss through online social media is demonstrated by the following actions:

1. Bringing in computer data with slanderous, insulting and impolite wording to the computerized system;
2. Bringing into the computerized system any data with violence character, false data, cheat data, and untrue data;
3. Bringing computer data which cause destruction to the national security, peace, social orderliness, fine culture and tradition of the nation;
4. Bringing computer data with the nature of persuading, exhorting and encouraging the people to resist the Government or to break solidarity;
5. Advertisement for trading of drug, war weapon, chemical weapon, human trafficking, prostitution, prostitution, trading of prostitute and other illegal activities;
6. Dissemination or forward computer data as specified in Article 11 and 14 of this law, including item 1, 2, 3, 4 and 5 of this Article.

Article 14 Dissemination of Pornography through the Computerized System

Pornography is data with clear content such as photo, moving picture, sound and video relating to sex organ and human sexual behavior.

Dissemination of pornography through the computerized system is to trade, distribute, transfer, advise and dissemination of data as specified in paragraph 1 above.

Article 15 Disturbance to Computerized System

Disturbance to computerized system is the following actions:

1. The application of computer program, virus or other apparatus in order to hinder or destroy the operation of computerized system;
2. Sending computer data or electronic mail through the concealment of address or origin of the sender in order to disturb and/or destroy the operation of computerized system.

Article 16 Falsification of Computerized System

The falsification of computerized system is the use of computer or computerized system and electronic apparatus in order to change the computer data through the following action:

1. Input data, changing data, falsifying electronic address or deleting data in the computerized system that cause any computerized data being changed from the original data on purpose;

2. Input and change data relating to financial transaction, trade, confidentiality and other data of individuals, legal entities, organizations without authorization;

3. Setting fake website in order to cheat, a deception to push the users of computerized system or the internet to provide the deposit account information, credit card code, internet application code, code for internet user and other data.

Article 17 Demolition of Computer Data

Demolition of computer data is to erase, edit and/or the changes in the computer data or data in the computerized system in order to make such data or such computerized system damages and differ from the original data.

Article 18 Business Operation relating to Cyber Crime Apparatus

Business operation relating to cybercrime apparatus is to build a new specific program, production, import, possession, trading, distribution, publication or recommendation of such apparatus, such as computer program or computer data design in order to build cybercrime.

Part III
Cybercrime Resistance and Prevention Movements
Chapter 1
Cybercrime Resistance and Prevention Activities

Article 19 Cybercrime Resistance and Prevention Activities

Cybercrime resistance and prevention activities are as follows:

1. Warning Notice;
2. Consultancy;
3. Emergency alert;
4. Solution procedures.

Article 20 Warning Notice

The Ministry of Post and Telecommunication is in charge of informing about any dangers occurred in the computer system and the internet such as a warning notice about fake website, malicious code, notifying about possible vulnerability in computer system, deceiving through e-mail and others.

Computer system service provider shall give a warning notice and determine the condition in the access to the computerized system in order to limit or not to authorize some types of service users to access to the computerized system.

Article 21 Consultancy

The Division of Post and Telecommunication shall provide consultancy and give advice on safeguarding method and technical solution to individuals, legal entities and organizations in order to reduce data loss, data disturbance, avoiding stopping the operation of computerized system, deterring the spread of computer virus and the attack to data in the computerized system.

Article 22 Emergency Alert

Individuals, legal entities and organizations (both local and foreign) who live, perform activities and use computerized system and/or computer data in the Lao PDR shall give crime related emergency alert which occurred to their computer system to Division of Post and Telecommunication as specified in Article 50 and 51 of this Law.

For common event, emergency alert shall be given to other relevant sectors.

Emergency Alert can be operated through the following methods:

1. Standard application form;
2. Telephone, fax, hot line;
3. Electronic mail;
4. Other methods.

Article 23 Solution Procedures

After receiving an emergency alert through the computerized system, the Ministry of Post and Telecommunication shall make consideration and send a notifying reply and give solution procedure within the period of five business days.

In case of necessity and urgency, the Ministry of Post and Telecommunication shall promptly carry on technical solution procedures in according to the emergency alert made by the person concerned.

In case of being notified about any events relating to some behaviors as specified in Article 11 and 13 of this law which affect the national security or the dignity of any individuals, relevant sectors (both in central and local level) shall consider replying on a case-by-case basis.

Chapter 2
Cybercrime Resistance and Prevention Activities

Article 24 Cybercrime Resistance and Prevention Activities

The cybercrime resistance and prevention activities are as follows:

1. Organizing propaganda and dissemination;
2. Training course;
3. Knowledge sharing on cyber safety;
4. Developing data protection activities;
5. Emergencies safeguarding;
6. Statistic Collection.

Article 25 Organizing Propaganda and Dissemination

The Ministry of Post and Telecommunication is the body in charge of developing manual, stickers, advertisement board, printing media and video relating to the safeguard, protection of computer crime, in coordination with other sectors and local administrative authority concerned to make propaganda and dissemination throughout the country.

Article 26 Training Course

Division of Post and Telecommunication shall collaborate with other sectors and relevant local administrative authority to organize training course for staff and officials concerned with regard to the cybercrime resistance and prevention activities, including both the investigation-interrogation work.

Article 27 Knowledge Sharing on Cyber Activities

The Ministry of Post and Telecommunication shall take initiative in collaborating with relevant sectors to set up specific measure to maintain the safety in computer system and to share knowledge on such measures to the society.

The Ministry of Post and Telecommunication shall take initiative in collaborating with the Ministry of Education and Sport to include the cyber safety subject in the teaching-studying curriculums from lower secondary upward.

Article 28 Developing Data Protection Activities

To guarantee the safety in the computerized system and the protection of computer data, the post and telecommunication sector, the security sector, service providers and data maintenance persons shall develop activities for sharing knowledge in terms of safety, computer system application to learn about the technique and data protection method within the state organization, private sector and education premises.

Article 29 Emergencies Safeguarding

The Post and Telecommunication sector shall be the body to safeguard emergencies through the monitoring, inspection, giving advice, warning notice, protection and response to the dangers occurred in the computer system.

Article 30 Statistic Collection

The Post and Telecommunication sector and the security sector shall collect statistic and build database relating to cybercrime and to make study and research on a regular basis in order to find out conditions and causes leading to cybercrime.

Chapter 3
The Centre for Deterring and Solving Computer Emergencies

Article 31 The Centre for Deterring and Solving Computer Emergencies

To enable the management, monitoring, inspection, resistance, restraint and elimination of crime, database protection, server system, computer data and the ability to link with the regional and international level, the state establishes the Centre for Deterring and Solving Computer Emergencies, in abbreviation " …….".

The Centre for Deterring and Solving Computer Emergencies is a ministry-equivalent organization under the organizational structure of the Ministry of Post and Telecommunication, having the role as a secretariat for such Ministry in deterring and solving computer emergencies.

The organization and activities of the Centre for Deterring and Solving Computer Emergencies shall have the rights and duties as follows:

1. To study and expand strategic plan, policy into its own plan, program and project before implement effectively;
2. To study and set up regulations on the management of the cybercrime resistance and prevention before propose to the Ministry of Post and Telecommunication;
3. To propagate, disseminate the laws and regulations relating to the cybercrime resistance and prevention;
4. To build, train, upgrade and develop personnel about the safety in computerized system;
5. To safeguard, monitor, inspect, instruct, warn and argue with computer emergencies as assigned;
6. To accept announcement, notice, and report any wrong action in the computerized system to relevant sectors;
7. To coordinate and cooperate with relevant sectors in the proceedings of computer system;
8. To notify the service users and data keepers to facilitate and provide data relating to cybercrime;
9. To contact, cooperate with foreign countries, regional and international levels with regard to cybercrime resistance and prevention activities as being assigned;

10. To summarize and report their own activities to the Ministry of Post and Telecommunication on a regular basis;

11. To exercise other rights and perform other duties as specified in the laws and regulations.

Part IV
International Cooperation
In Cybercrime Resistance and Prevention

Article 33 Basic Principles in International Cooperation

The international cooperation in cybercrime resistance and prevention between the Lao PDR authority and foreign countries shall abide by the principles of mutually respecting independency; sovereignty and full territory of each other, no interference to each other internal tasks, maintaining equality and mutual interests and in conformity with the international convention and treaty in which the Lao PDR is a partner country.

Article 34 Technical Cooperation

The international cooperation in technical aspect in order to deter and solve emergencies of the computerized system shall have the main contents as follows:

1. Exchanging of technical information, including the research on standard relating to standards for combatting and deterring emergencies of computerized system;

2. Calming down or notifying to stop any harmful act to the computerized system;

3. Coordination with service providers in foreign countries regarding the use of online social media with the content as specified in Article 13 of this law;

4. Mutual assistance in safeguarding, deterring and solving emergencies on computerized system in important event, such as conference at national level, regional and international levels including various festivals.

Article 35 Mutual Legal Assistance

Mutual legal assistance conducts through the request to carry out investigation-interrogation, by applying deterring measures, issuing instruction to maintain and protect computer data, including the data circulated through computerized system, conducting research, indicating and pointing out offender, confiscation or seizure of equipment or apparatus that use and relating to any offense, asking additional evidence relating to wrong act and trans-national crime. The mechanism and procedures of mutual legal assistance shall be abide with the relevant laws and regulations of the Lao PDR, international convention and treaty in which the Lao PDR if the partner country.

Article 36 Content of Request for Mutual Legal Assistance

A request for mutual legal assistance shall have the content as follows:

1. Objectives, necessity and the actual status of the request;

2. Important information for certifying, monitoring and indicating cybercrime person;

3. Make a brief summary of computer data or data circulated through computerized system that requires special storage or protection;

4. Legal reference regarding the action of accused person;

5. Authority or relevant officials can request for additional information from any country requesting legal assistance.

Article 37 Confidentiality

Lao PDR authority with related rights shall protect keep confidential the secret of the country requesting legal assistance.

Article 38 Refusal of Request

Lao PDR authority with related rights may refuse any request for mutual legal assistance if such request is in contradiction with the basic principles of the international cooperation as specified in Article 33 of this law and other relevant laws of the Lao PDR.

Part V
Prohibitions

Article 39 General Prohibitions

Individuals, legal entities or organizations are prohibited from the following behaviors:

1. Have behaviors as specified in Article 8 of this law;
2. Organize propaganda to destroy political regime in order to create social unrest;
3. Destroy or cause damages to electronic equipment, computer and other facilities while sharing information through the computerized system;
4. Have complicity with any individuals in order to disseminate pornographies through online social media;
5. Claim for, ask for, give and accept bribes;
6. Having other behaviors that violate the laws and regulations.

Article 40 Prohibitions for Service Providers

Service providers shall be prohibited from the following behaviors:

1. Delete any data circulated through the computerized system prior to ninety days in connecting case and before three hundred sixty-five days in non-connecting case;
2. Delete data of computerized system user which cause the loss before ninety days;
3. Provide incorrect data to officials and relevant staffs;
4. Disclose the information of service users without authorization;
5. Build condition or facilitate the cybercrime activities;
6. Have other behaviors that violate the laws and regulations.

Article 41 Prohibitions for Officials and relevant Staffs

Officials and relevant staffs are prohibited from the following behaviors:

1. Disclose privacy of the state, official, individuals, legal entities or organizations through the computerized system;
2. Disclose computer access code and specific safeguarding measures of its sectors;
3. Hand over to other persons any computer data, data circulated through the computerized system or data of service users, except handing-over that benefits case proceedings such as to implement court sentences or in case that authorization is made from case proceeding authority;
4. Delay, hinder and falsify document regarding the cybercrime information;
5. Make use of position for personal interest, interest of family and clan;
6. Abandon responsibilities assigned by organizations;
7. Have other behaviors that violate the laws and regulations.

Part VI
Investigation-Interrogation of Computerized System Cases

Article 42 Reason Leading to Opening of Investigation-Interrogation

The reasons leading to opening of investigation-interrogation are as follows:

1. When having announcement, reporting, petition made by individuals, legal entities or organizations regarding cybercrime behaviors;
2. Turning oneself in by offender;
3. Discovering clue, information, evidence of behavior as specified in Article 8 of this law.

Article 43 Steps of Case Investigation-Interrogation through Computerized System

Investigation-interrogation of case through computerized system shall comply with the steps below:

1. Announcement, reporting or litigation;
2. Opening of investigation-interrogation;
3. Conducting of investigation-interrogation;
4. Summarizing investigation-interrogation and completion of case file.

Article 44 Announcement, Reporting or Petition

Announcement, reporting or petition regarding cybercrime offense shall be made or submitted to the police investigation-interrogation authority or to the Public Prosecution Authority.

The police investigation-interrogation authority or the Public Prosecution Authority shall consider making announcement, reporting or petition no later than fifty business days from the date of receiving announcement, report or petition onward. In case of complexity, such consideration shall not exceed ten business days.

Article 45 Opening of Investigation-Interrogation

In case of having strong information regarding cybercrime, the head of the police investigation-interrogation authority or the head of the public prosecution authority shall issue an order to open the investigation-interrogation within the scope of its rights and responsibilities as specified in the Law on criminal procedures.

In case of necessity, urgency and availability of data proving of any cybercrime plan or action, the head of police investigation-interrogation authority or the head of the Public Prosecution shall issue an instruction/order to keep and protect computer data or data circulated through the computerized system.

The service provider or data management sector shall have an obligation to keep and protect such data in good form until the end of the case proceedings in order to guarantee that there are no changes or loss to the data.

Article 46 Investigation-Interrogation Proceedings

The policy investigation-interrogation authority or the Public Prosecution Authority shall collaborate with the Post and Telecommunication Sector and other relevant sectors to conduct a search for data, evidence and the background of cybercrime to be used as reference for the investigation-interrogation process.

The investigation-interrogation proceedings for computer related cases shall apply the investigation-interrogation method, restraining measures and time limit for the investigation-interrogation as specified in the Law on Criminal Procedures.

Article 47 Summarizing of Investigation-Interrogation and Completion of Case File

After ending the investigation-interrogation by police officer, if there is no strong evidence proving that such infringement is offense on computerized system, the investigation-interrogation

authority shall summarize and complete case file in order to submit to the Public Prosecution Authority for consideration and lodge a lawsuit to the court.

In case that the Public Prosecution Authority is the body conducting investigation-interrogation, such authority shall summarize, complete case file, issue an indictment order and statement to the court for consideration making case sentence in accordance with the law.

Part VII
Management and Inspection
Chapter 1
Management

Article 48 Management Authority

The Government is in charge of managing the cybercrime resistance and prevention activities in a centralized and uniformed manner throughout the country by assigning the Ministry of Post and Telecommunication to directly responsible for and to take initiative in collaborating with the Ministry of National Defense, Ministry of Public Security, Ministry of Information, Culture and Tourism, Ministry of Sciences and Technology, other ministries and local administration concerned.

The Authority in charge of the management of cybercrime resistance and prevention activities comprises of:

1. Ministry of Post and Telecommunication;
2. Division of Post and Telecommunication of provincial, city level;
3. Office of Post and Telecommunication at district, municipality level.

Article 49 Rights and Duties of the Ministry of Post and Telecommunication

In the management of cybercrime prevention activities, the Ministry of Post and Telecommunication shall have the rights and duties as follows:

1. To study, build strategic plan, policy, law related to cybercrime resistance and prevention activities in order to propose to the Government for consideration;
2. To propagate, disseminate the laws and regulations relating to cybercrime resistance and prevention activities across the country;
3. To guide capacity building, training, upgrading and development of personnel on the safety of the computerized system;
4. To guide the safeguarding, monitoring, inspect, advise, warn and response to computerized system emergencies;
5. To coordinate with ministries, authority concerned in performing activities related to cybercrime resistance and prevention;
6. To contact, cooperate with foreign countries, regional and international levels about cybercrime resistance and prevention;
7. To brief and report its activities to the Government on a regular basis;
8. To exercise such other rights and to perform such other duties as specified in the laws and regulations.

Article 50 Rights and Duties of the Division of Post and Telecommunication at Provincial, City Level

In the management of cybercrime resistance and prevention activities, the Division of Post and Telecommunication at provincial, city level shall have the rights and duties based on its scope of responsibilities as follows:

1. To propagate, disseminate strategic plan, policy, laws, regulations relating to cybercrime resistance and prevention activities before implementation;

2. To set up plan for capacity building, training, upgrading and development of personnel concerning cybercrime resistance and prevention activities then to propose to higher authority;

3. To accept notification on emergencies in computer system then to report to the Center for deterring and solving computer emergencies;

4. To announce, report on wrong act in computerized system to the investigation-interrogation authority and the public prosecution authority at provincial, city level;

5. To coordinate and cooperate with the investigation-interrogation authority or public prosecution authority at provincial, city level in order to conduct case proceedings on computerized system;

6. To notify service provider, data keeper to give convenience and provide data relating to wrong act in computerized system;

7. To coordinate with other relevant sectors to perform activities related to cybercrime prevention;

8. To coordinate, cooperate with the computer emergencies deterring and solving center of the Ministry of Post and Telecommunication;

9. To collect cybercrime statistic;

10. To coordinate, communicate and cooperate with foreign countries, regional and international levels regarding the cybercrime resistance and prevention activities as being assigned;

11. To summarize and report its performance of activities to the Ministry of Post and Telecommunication and to local administrative authority at provincial, city levels on a regular basis;

12. To exercise such other rights and to perform such other duties as specified in the laws and regulations.

Article 51 Rights and Duties of the Post and Telecommunication Office of District/Municipality

In the management of cybercrime resistance and prevention activities, the Post and Telecommunication Office of District/Municipality shall have the rights and duties based on its scope of responsibilities as follows:

1. To propagate, disseminate strategic plan, policy, laws, regulations relating to cybercrime resistance and prevention activities before implementation;

2. To set up plan for capacity building, training, upgrading and development of personnel concerning cybercrime resistance and prevention activities then to propose to its next higher authority;

3. To accept notification on emergencies in computer system then to report to the Center for deterring and solving computer emergencies;

4. To announce, report on wrong act in computerized system to the investigation-interrogation authority and the public prosecution authority at regional level;

5. To coordinate and cooperate with the investigation-interrogation authority or public prosecution authority at regional level in order to conduct case proceedings on computerized system;

6. To coordinate with other relevant sectors to perform activities related to cybercrime resistance and prevention;

7. To collect cybercrime statistic;

8. To summarize and report its performance of activities to the Division of Post and Telecommunication and to local administrative authority at district/municipal levels on a regular basis;

9. To exercise such other rights and to perform such other duties as specified in the laws and regulations.

Article 52 Rights and Duties of other Sectors and Local Administrative Authority

In the management of cybercrime resistance and prevention activities, other relevant sectors such as national defense, public security, information and tourism, sciences and technology and local

administrative authority shall have the rights to participate, cooperate in cybercrime resistance and prevention, report and provide the information relating to such crime based on the scope of their responsibilities.

Chapter 2
Inspection

Article 53 Inspection Authority

The Cybercrime Resistance and Prevention Activities Inspection Authority comprises of:

1. The Internal Inspection Authority which is the same authority as the Authority in charge of the management of cybercrime resistance and prevention activities as specified in Article 48 of this law;
2. The External Inspection Authority which includes the National Assembly, the State Audit Authority, the Government Inspection Anti-Corruption Authority, the Lao Front for National Construction and the mass organization.

Article 54 Content of Inspection

The content of inspection of cybercrime resistance and prevention activities are as follows:

1. The implementation of strategic plan, policy, law and regulations related to cybercrime resistance and prevention activities;
2. The organization and activities of the Authority in charge of the management of cybercrime resistance and prevention activities;
3. The exercise of international convention and treaty relating to cybercrime resistance and prevention activities in which the Lao PDR is a partner country.

Article 55 Form of Inspection

The inspection shall be conducted through the following forms:

1. Inspection done on a regular basis;
2. Inspection done through advance notice;
3. Inspection done all of a sudden.

The inspection done on a regular basis is an inspection that proceeds regularly in according to the plan and with accurate timeframe.

The inspection done through advance notice is an out-of plan inspection when necessary by notifying in advance to the inspection target.

Inspection done all of a sudden is an urgent inspection in which the inspection target is not informed in advance.

The inspection must be strictly conducted in conformity with the laws and regulations.

Part VIII
Rewards for Persons with Outstanding Performance and Measures against Violators

Article 56 Rewards for Persons with Outstanding Performance

Individuals, legal entities or organizations who show outstanding performance in implementation of this law, especially in reporting, giving cooperation, providing information relating to any cybercrime behavior shall be commended and receive other rewarding policies according to the regulation.

Article 57 Measures against Violators

Individuals, legal entities or organizations who violate this law, especially the infringement of any prohibitions, shall be subject to re-education, warning, disciplinary measures, fine, compensating for civil loss or criminal punishment based on the seriousness of the case as specified in the laws and regulations.

Article 58 Re-educational Measures

Individuals, legal entities or organizations who violate this law which is the first violation and that causes minor damages shall be subject to re-education and warning.

Article 59 Disciplinary Measures

Relevant staff and officials who violate this law that is not considered criminal offence shall be subject to disciplinary measures according to the following cases:

1. To be reprimanded and warned of such offence according to the regulation and be recorded in his or her personal profile;
2. To be suspend the promotion, salary increase and commendations;
3. To be removed from one's post and transferred to a lower one;
4. To be dismissed from the public service without any incentive remuneration.

In addition, the person shall return to the organization all of the assets acquired illegally from his/her performance of duties.

Article 60 Fine Measures

Individuals, legal entities or organizations who violate this law shall be fined according to the following cases:

1. Provide incorrect information to concerned staff and officials that cause no damages to anyone;
2. Fail to provide information within the time limit given by concerned staff of officials;
3. Delete data in computerized system or computer data of other persons without any authorization;
4. Other cases as specified in the laws and regulations related to administrative violation.

Rates of fine for each case are specified in a separate regulation.

Article 61 Civil Measures

Individuals, legal entities or organizations who violate this law which cause damages to other persons shall compensate for any damages incurred.

Article 62 Penal Measures

Individuals who committed a crime in the following cases shall be subject to punishments as follows:

1. Revelation of computer access protection measures shall be subject to a deprivation of liberty punishment from one month to one year and shall be imposed with a fine from 1,000,000 kips to 4,000,000 kips.
2. Unauthorized access to computerized system shall be subject to a deprivation of liberty punishment from 3 months to one year and shall be imposed with a fine from 2,000,000 kips to 5,000,000 kips;
3. Censor of content, photo, moving picture, sound and video without authorization shall be subject to a deprivation of liberty punishment from three months to two years and shall be imposed with a fine from 3,000,000 kips to 10,000,000 kips;

4. Stealing data in the computerized system without authorization shall be subject to a deprivation of liberty punishment from three months to three years and shall be imposed with a fine from 4,000,000 kips to 20,000,000 kips;

5. Incurring damages through online social network shall be subject to a deprivation of liberty punishment from five months to three years and shall be imposed with a fine from 4,000,000 kips to 20,000,000 kips;

6. Publication of pornography through computerized system shall be subject to a deprivation of liberty punishment from one year to five years and shall be imposed with a fine from 5,000,000 kips to 30,000,000 kips;

7. Interference of computerized system shall be subject to a deprivation of liberty punishment from one to five years and shall be imposed with a fine from 5,000,000 kips to 30,000,000 kips;

8. Falsification of computer data shall be subject to a deprivation of liberty punishment from one to five years and shall be imposed with a fine from 5,000,000 kips to 30,000,000 kips;

9. Destruction of computer data shall be subject to a deprivation of liberty punishment from three to five years and shall be imposed with a fine from 10,000,000 kips to 50,000,000 kips;

10. Operation of business related to cybercrime apparatus shall be subject to a deprivation of liberty punishment from three years to five years and shall be imposed with a fine from 10,000,000 kips to 50,000,000 kips.

Part IX
Final Provision

Article 63 Implementation

The Government of the Lao People's Democratic Republic is implementing this law.

Article 64 Effectiveness

This law shall come into effect from the date that the President of the Lao People's Democratic Republic issued a promulgation decree and after fifteen days of being posted in an official gazette.

Any regulations, provisions that contradict with this law shall be annulled.

President of the National Assembly

[Seal and signature]

Pany Yathortou