Kingdom of Cambodia
Nation Religion King
******

Cybercrime Law

Draft V.1

Unofficial Translation to English

Contact Person: Mr. OU Phannarith
Permanent Member
Email: phannarith-ou@nida.gov.kh
Tel: (855) 92 33 55 36

Draft by Cybercrime Law Formulation Working Group of Council of Ministers

Table of Content

Chapter 1 – General Provision

Article 1: Purpose

This law has a purpose to determine education, prevention measures and combat all kinds of offense commit by computer system.

Article 2: Objective

This law has objectives:

- Ensure the implementation of law, anti-cybercrime and combating all kinds of offense commit by computer system
- Ensure safety and prevent all legitimate interest in using and developing technology

Article 3: Scope

This law is applicable to all offenses in this law in the following situation:

- Offense committed inside Kingdom of Cambodia or
- Offense committed inside or outside Kingdom of Cambodia and effect to legal and natural person or interest of Kingdom of Cambodia.

Article 4: Terms and Definition

The technical terms in this law are as follow:

1. *"computer system"* means any device or assembly of interconnected devices or that are in an operational relation, out of which one or more provide the automatic data processing by means of a computer program.

2. *"automatic data processing"* is the process by means of which the data in a computer system are processed by means of a computer program.

3. "Computer Program" means a sum of instructions expressed in letters, or codes, or illustrations, or in any other possible forms, once incorporated in a computer, which has its aim to accomplish a task or particular result by means of a computer or through an electronic procedure capable of information processing.

4. "computer data" are any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function.

5. "Content" refers to electronic form including text, images, graphics, animation, symbols, voices, and video.

6. Serivce providers refer to:

   1. any natural or legal person offering the users the possibility to communicate by means of a computer system;

2. any other natural or legal person processing or storing computer data for the persons mentioned in paragraph 1 and for the users of the services offered by these;

7. "traffic data" are any computer data related to a communication by means of a computer system and generated by this, which represent a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication.

8. "security measures" refers to the use of certain procedures, devices or specialised computer programs by means of which the access to a computer system is restricted or forbidden for certain categories of users;

9. "competent authority" refers to the Secretariat of National Committee on Anti-Cybercrime or any competent authority in other countries.

10. "Website" refers to place on the Internet, which you can find any information.

11. A person acts without right in the following situations:

a) is not authorised, in terms of the law or a contract;
b) exceeds the limits of the authorisation;
c) has no permission from the competent natural or legal person to give it, according to the law, to use, administer or control a computer system or to carry out scientific research in a computer system.

Chapter 2 – National Anti-Cybercrime Committee (NACC)

Article 5: Establishment of National Anti-Cybercrime Committee (NACC)

The National Anti-Cybercrime Committee is established and the abbreviation is NACC.

Article 6: Composition of NACC

The NACC shall composed of the following:

1.	Prime Minister		Chairman
2.	Deputy Prime Minister, Minister in Charge of Council of Ministers		Deputy Chairman
3.	Secretary of State	Ministry of Interior	Member
4.	Secretary of State	Ministry of Foreign Affair	Member
5.	Secretary of State	Ministry of Information	Member
6.	Secretary of State	Ministry of Posts and Tel	Member
7.	Secretary of State	Ministry of Justice	Member
8.	General Commissioner	National Police	Member
9.	Representative	Anti-Terrorism	Member
10.	Representative	Council of Jurist	Member
11.	Representative	Ecosocc	Member

12. Representative	Chamber of Commerce	Member
13. Secretary General	NiDA	Member
14. Secretary General	NACC	Permanent Member

The actual person of NACC will be determined in separate Royal Decree.

Article 7: Duties of NACC

The National Anti-Cybercrime Committee has the following duties:

- Devises strategies, action-plans, and related programs in securing cyber and information grid for the Royal Government of Cambodia.
- Advises and recommend course of actions to the General Secretariat of the National Anti-Cybercrime Committee
- Supervises work-flows and course of action-plans implementations of the General Secretariat of the National Anti-Cybercrime Committee
- Issues findings and appropriate recommendations for ministries and departments to ensure the security of cyber and information grid of the Royal Government of Cambodia.
- Provides cyber and information grid security report for the nation to the Royal Government bi-semester and annually.
- Performs duties directed by the Royal Government of Cambodia.

Article 8: General Secretariat of NACC

NACC has one General Secretariat as an operation unit. General Secretariat of NACC is lead by one Secretary General and a number of Deputy Secretary General as assistance.

Secretary General and Deputy Secretary General are appointed by Royal Decree.

The organization and function of the General Secretariat is defined by Sub Decree.

Article 9: Duties of The Secretary General of NACC

The General Secretariat of the NACC has the following duties:

- Enforces laws, orders, and laws related to cyber-crime.
- Investigates, supervises, and researches including develops measures relating to cyber-criminal activities.
- Leads, manages, prevents, interrupts, and counter strikes against any cyber-criminal activities directed toward the Kingdom of Cambodia.
- Develops regulations, standardization, and strategic plans related to cyber-crime.

- Supervises, evaluates, and certifies security qualities meeting standards for computers systems, network architecture, computer programs, and information technology (cyber) services.
- Enforces, publicizes, educates, and elevates the nation's knowledge in information technology.
- Work in cooperation with ministries, organizations of the Royal Government of Cambodia, national organizations, regional organizations, and international communities in order to investigate, supervise, research, manage, prevent, interrupt, and counter strike against cyber-criminal activities.
- Appoints, replaces, and manages, or requests for appointment and replaces government's employees under the direction of the General Secretariat of NACC.
- Supervises and develops the NACC's yearly budget for submission.
- Writing all official reports of all related for the NACC and the Royal Government of Cambodia.
- Performs duties directed by the NACC and the Royal Government of Cambodia.

Article 10: Officials of the General Secretariat of NACC

The officials of the Secretariat General of NACC include the persons appointed or transferred or assigned to work for the Unit and the contractual officials. These officials have to follow the provisions of the law and legal norms in force.

The Secretary General of the NACC can recruit local or international experts, specialists or researchers, on the voluntary or contractual basis, to provide technical expertise on anti-cybercrime.

Article 11: Branches of General Secretariat of NACC

The Secretariat General of NACC may have its offices in the Capital and all provinces of the Kingdom of Cambodia to serve as its branches. The Offices for General Secretariat of NACC perform their work under the leadership of Secretary General of General Secretariat of NACC. The Office for General Secretariat of NACC is led by one chief and a number of deputy chief as his assistants.

Article 12: Budget and Resources for NACC

The NACC has a separate budget package for its operation and the package is within the budget package of the Office of the Council of Ministers.

The NACC receives needed resources from the Royal Government and has the right to receive donations or assistance from national and international organizations.

Chapter 3: Procedure Provision

Article 13 - Procedure for Cybercrime Offence

Procedure for Cybercrime offenses, which is stated in this law, shall be implemented as stated in the penal code procedure if there is no separate procedure in this law.

Article 14 - Officials competent to investigate Cybercrime offence

Secretary General, Deputy Secretary General and officials of National Anti-Cybercrime Committee who gain an advantage as judicial police official are empowered to investigate cybercrime offenses that are stipulated in this law and those in the panel code.

Other persons or units that are aware of cybercrime offenses are stipulated in this law and cybercrime offenses stated in the panel code share make complaints to the National Anti-Cybercrime Committee.

Article 15 – Appointment of National Anti-Cybercrime Committee officials as judicial police

Secretary General and Deputy Secretary General of National Anti-Cybercrime Committee are legally entitled to a status as judicial police officials in order to perform their duties.

Officials of National Anti-Cybercrime Committee may be entitled to status as judicial police officials in accordance with the provisions in the penal procedure code.

The Secretary General of National Anti-Cybercrime Committee takes charge of preparing list of officials of National Anti-Cybercrime Committee who are entitled to status as judicial police officials through Prakas of the Minister of Justice.

Article 16 – Investigation Power of NACC

Officials of National Anti-Cybercrime Committee who are appointed as judicial police take charge of investigating cybercrime offences. If during the course of a cybercrime offence, investigation different offenses are found whose facts are related to the offence being investigated by National Anti-Cybercrime Committee, officials of National Anti-Cybercrime Committee shall make complaint to competence authority.

Secretariat of National Anti-Cybercrime Committee can not investigate other offences except ones unless with the court order.

The court can order National Anti-Cybercrime Committee to undertake forensic inquiries in order to facilitate the work of the court.

In the framework of these investigations and contradictory to article 85 (power of judicial police officials in flagrant offence investigation), article 91 (searching), article 94 (subpoena in the case of flagrant offence investigation) and the article 114 (subpoena for preliminary investigation) of the code of criminal procedure, the Secretary General of National Anti-Cybercrime Committee or officially assigned representative has the duty to lead, coordinate and control the mission of those officials instead of the role of prosecutor to the point of arresting a suspect.

After the arrest, prosecutor exercises his power as stated in the code of criminal procedure.

At the end of each investigation, the National Anti-Cybercrime Committee shall submit all facts to the prosecutor for further action in conformity with the provisions of the code of criminal procedures.

Article 17: Preservation of Computer Data and Traffic Data

1. In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.

2. During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.

3. The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.

4. The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.

5. In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.

6. Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

Article 18: Copying Data

1. Within the term provided for at art. 17 paragraph (3), the prosecutor, on the basis of the motivated authorisation of the prosecutor specially assigned by the general prosecutor of the office related to the Court of Appeal or, as appropriate, by the general prosecutor of the office related to the Supreme Court, or the court orders on

the seizing of the objects containing computer data, traffic data or data regarding the users, from the person or service provider possessing them, in view of making copies that can serve as evidence.

2. If the objects containing computer data referring to the data for the legal bodies in order to make copies, the prosecutor mentioned in paragraph (1) or court orders the forced seizure. During the trial, the forced seizure order is communicated to the prosecutor, who takes measures to fulfil it, through the criminal investigation body.

3. The copies mentioned in paragraph (1) are achieved by the technical means and the proper procedures to provide the integrity of the information contained by them.

Article 19: Searching and Seizing Computer Data

1. Whenever for the purpose of discovering or gathering evidence it is necessary to investigate a computer system or a computer data storage medium, the prosecutor or court can order a search.

2. If the criminal investigation body or the court considers that seizing the objects that contain the data referred to at paragraph (1) would severely affect the activities performed by the persons possessing these objects, it can order performing copies that would serve as evidence and that are achieved according to art. 18, paragraph (3).

3. When, on the occasion of investigating a computer system or a computer data storage medium it is found out that the computer data searched for are included on another computer system or another computer data storage medium and are accessible from the initial system or medium, it can be ordered immediately to authorize performing the search in order to investigate all the computer systems or computer data storage medium searched for.

Article 20: Condition and Safeguard

1. The access to a computer system, as well as the interception or recording of communications carried out by means of computer systems are performed when useful to find the truth and the facts or identification of the doers cannot be achieved on the basis of other evidence.

2. The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed.

3. The authorisation referred to at paragraph (2) is given for 30 days at the most, with the extension possibility under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 4 months.

4. Until the end of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons against whom the measures referred to in paragraph (1) are taken.

5. The procedures of the Criminal procedure Code regarding the audio or video recordings are applied accordingly.

Chapter 4: Offences

Article 21: Illegal Access

1. The access without right to a computer system is an offence shall be sentenced from 06 months to 03 years and fined from one million Riel (1,000,000) to six million Riel (6,000,000).

2. It is an offence where the act provided in paragraph (1) is committed with the intent of obtaining computer data, shall be sentenced from 06 months to 05 years and fined from one million Riel (1,000,000) to ten million Riel (10,000,000).

3. It is an offence where the act provided in paragraphs 1-2 is committed by infringing the security measures, shall be sentenced from 03 years to 12 years and fined from six million Riel (6,000,000) to twenty four million Riel (24,000,000).

Article 22: Data Espionage

1. Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be sentenced from 01 years to 03 years and fined from two million Riel (2,000,000) to six million Riel (6,000,000).

2. Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.

Article 23: Illegal Interception

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data, shall be sentenced from 02 years to 07 years and fined from four million Riel (4,000,000) to fourteen million Riel (14,000,000).

Article 24: Data Interference

The alteration, deletion or deterioration of computer data or restriction to such data without right is an offence, shall be sentenced from 02 years to 07 years and fined from four million Riel (4,000,000) to fourteen million Riel (14,000,000).

Article 25: Unauthorized Data Transfer

The unauthorized data transfer from a computer system or by means of a computer data storage medium is an offence shall be sentenced from 03 years to 12 years and fined from six million Riel to twenty four million Riel (24,000,000).

Article 26: System Interference

The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data, shall be sentenced from 03 years to 15 years and fined from six million Riel to thirty million Riel.

Article 27: Child Pornography

1. Any person when committed intentionally and without right, the following conduct:

    a) producing child pornography for the purpose of its distribution through a computer system;
    b) offering or making available child pornography through a computer system;
    c) distributing or transmitting child pornography through a computer system;
    d) procuring child pornography through a computer system for oneself or for another person;
    e) possessing child pornography in a computer system or on a computer-data storage medium.

Shall be sentenced from 01 year to 03 years and fined from two million Riel (2,000,000) to ten million Riel (10,000,000).

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct;
b) a person appearing to be a minor engaged in sexually explicit conduct;
c) realistic images representing a minor engaged in sexually explicit conduct.

Article 28: Contents and Websites

Any persons who engage in activities set forth in the followings:

1. Establishing contents that deemed to hinder the sovereignty and integrity of the Kingdom of Cambodia is a punishable offense of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).
2. Publications that deemed to incite or instigate the general population that could cause one or many to generate anarchism is punishable of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).
3. Publications or continuation of publication that deemed to generate insecurity, instability, and political cohesiveness is a punishable office of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).

4. Publications or continuation of publication that deemed to be non-factual which slanders or undermined the integrity of any governmental agencies, ministries, not limited to departments, federal or local levels, is a punishable offense of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).
5. Publications that deemed damaging to the moral and cultural values of the society as stated herein:
    a. Information that incites or instigates prejudice on race or clans, color, gender, language, religion, beliefs or political views, origin of race or nationality, and not limited to levels or class in society.
    b. Writings or pixilation that deemed to display inappropriate activities of persons, copulations between humans or animals, or devalue the moral of family values and pixilation that deemed to display domestic violence
    c. Manipulation, defamation, and slanders
    d. Drawings, pictorials, or pixilation that deemed to slander or defame human beings or commoners of the state performing activities unbecoming, with animals of any species is punishable of incarceration from one to three years and fined 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).

Publicizing with the intent to threatened and commit a crime not limited to one form of felonies or other felonies with the intent to interrupt a person or persons well-beings is punishable of incarceration from one to three years and fined 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels). In the case of with the intent to threaten shall be treated as such law that is currently being enforced.

Article 29: Intellectual Property Right and Related Rights

Offences related to Intellectual Property Right and Related Rights need to implement it base on the existing Copyright and Related Right Law of Kingdom of Cambodia.

Article 30: Computer Related Fraud

The causing of a loss of property to another person by inputting, altering or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another shall be sentenced from 03 years to 12 years and fined from six million Riel (6,000,000) to twenty four million Riel (24,000,000).

Article 31: Computer Related Forgery

The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to such data, resulting in inauthentic data, with the intent to be used for legal purposes, is a criminal offence and shall be punished with imprisonment from 2 to 7 years.

Article 32: Misuse of Device

1. Any person when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 21 through 32;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 21 through 32; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 21 through 32. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Shall be sentenced from 1 year to 6 years and fined from two million Riel (2,000,000) to twelve million Riel (12,000,000).

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 21 through 32 of this Convention, such as for the authorised testing or protection of a computer system.

Article 33: Attempt

Attempt to commit a misdemeanor as stated in Article 427 (Accessing or Maintaining Access to Automated Data Processing System), Article 428 (Act of Obstructing the Operations of Automated Data Processing System), Article 429 (Fraudulent Introduction, Deletion or Modification of Data), Article 430 (Participation in Group or a Agreement to prepare for the commission of Offences) of Criminal Code and Article 21 (Illegal Access), Article 22 (Data Espionage), Article 23 (Illegal Interception), Article 24 (Data Interference), Article 25 (Unauthorized Data Transfer), Article 26 (System Interference), Article 27 (Child Pornography), Article 28 (Contents and Websites), Article 29 (Intellectual Property Rights and Related Rights), Article 30 (Computer Related Fraud), Article 31 (Computer Related Forgery) and Article 32 (Misuse of Device) of this law shall face the same punishment as misdemeanor.

Article 34: Accessory Penalty applicable to certain Cybercrime Offences

For the felonies and the misdemeanors described in this present chapter, the following additional penalties may be pronounced:

1. the deprivation of civil rights;
2. the prohibition against pursuing a profession during which time the crime was committed in course of or during the occasion of pursuing of this profession;
3. the confiscation of any instruments, materials or any objects which have been used to commit the offense or were intended to commit the offense;
4. the seizure of the objects or funds with which the offense was funded and/or carried out ;
5. the confiscation of incomes or properties earned/generated by the offense;
6. the seizure of the utensils, materials and the furniture garnishing a premise in which the offense was committed;
7. the confiscation of one or several vehicles belonging to the convicted person;
8. the posting of the decision of the sentence for 02 (two) months maximum;
9. the publication of the decision of the sentence in the newspapers;
10. Broadcasting of the decision of the sentence by all means of audio-visual communications for 08 (eight) days maximum.

Article 35: Accessory Penalty Applicable to Certain Legal Entities

The legal entity that commits offences as stated from article 21 to 32 in this law shall be subjected to fine of …… to ……. and face accessory penalties as follows:

1. Dissolution
2. Placement under the court watch
3. Baring of operation of an activity or activities
4. Expulsion from public procurement
5. Prohibition on public saving appeal
6. Prohibition of the business establishment open to the public or used by the public
7. Confiscation of instrument, material or any objects which are used to commit offence or aimed to commit offence
8. Confiscation of objects or funds which are subject of committing offence
9. Confiscation of proceeds, materials and furniture in building where an offence is committed
10. Posting of conviction judgment
11. Publication of the conviction judgment on print media or the announcement on non-print media outlets

Chapter 5: Mutual Legal Assistance, International Cooperation and Extradition

Article 36: Extradition Provision

Provisions of Chapter 2, content 1, part/section 9 of Penal Procedure Code shall be applicable in terms of the extradition of the case related to cybercrime offenses.

Article 37: Mutual Legal Assistance

In the case of cyber-crime offences, the court authority of the Kingdom of Cambodia may delegate power to competent court authority of any foreign state and may also obtain power from the court authority of any foreign state, in order to:

1. Collect evidence, proof or answer, response through court means
2. Inform about documents of the court
3. Search, arrest, and confiscate
4. Examine objects and crime scene
5. Providing information and exhibit
6. Issue original process-verbal or its authentic copies and dossier, including bank statement, accounting transactions, records of concerned institution, records of concerned company and trade records, as well as authentic and private documents;
7. Identify or provide expert witnesses and others, including detainees who agree to assist in the investigation or participate in the legal proceedings.
8. Identify or seek resources, property, equipment, and materials that derive from offence and offence means.
9. Place under temporary holding the products and properties obtained from corruption offences as well as equipment, materials being used or kept for committing offences.
10. Enforce the decision of confiscation, seizure or repatriation of products, properties, equipment, material derived from offence.
11. Order to confiscate all objects as stated above.
12. Inform about the criminal charge.
13. Interrogate the accused based on criminal procedure.
14. Find out and identify witnesses and suspects.

Article 38: Mutual Legal Assistance Procedure

Procedures for Implementing mutual legal assistance shall be in agreement with the principles stated in treaties or bilateral and multi-lateral agreement, and national law in force.

Chapter 6: Final Provision

Article 39: Abrogation

Any provisions that contradict with this law shall be abrogated.

Article 40: Law Implementation

This law shall go into effect 12 (twelve) months after the promulgation.

****