Memorandum of Principle and Rationale of [Draft] National Cybersecurity Act B.E. …

Principle

To legislate on the maintenance of national Cybersecurity.

Rationale

The use of Information Technology (IT) in daily transactions and communications has led to an environment susceptible to cyber threats and crimes capable of causing widespread impact, which is now exacerbated and causing damages both on the personal and national levels. As a result, the protection and tackling of cyber threats or risks requires swiftness and co-operation with all relevant agencies in order to ensure timely protection and tackling, and to continuously maintain Cybersecurity. In order for Thailand to be able to appropriately protect, prevent, and tackle circumstances of cyber threats which may impact or jeopardise the service or application of computer network, internet, telecommunications network, or regular service of satellites in ways that affect national security, including military security, domestic peace and order, and economic stability; and to ensure the swiftness and uniformity of such execution, a Committee is set up to effectively and efficiently determine measures on national Cybersecurity.

[Draft]
National Cybersecurity Act B.E. …

…….

Section 1 This Act is called "The National Cybersecurity Act B.E. …"

Section 2 This Act shall come into force after the expiration of 180 days from the date of its publication in the Government Gazette.

Section 3 In this Act:
"Cybersecurity" means measures and operations that are conceived in order to maintain national Cybersecurity, enabling it to protect, prevent or tackle circumstances of cyber threats which may affect or pose risks to the service or application of computer network, internet, telecommunications network, or the regular service of satellites in ways that affect national security, which includes military security, domestic peace and order, and economic stability.

"State agency" means any ministry, department, State division otherwise called and having equivalent status of a department, regional authority, local authority, public organisation, state enterprise, and agency set up by an Act or a Royal decree, and this includes any juristic person, body of persons or person having the power to act in the government's operation in any case.

"Officials" means persons appointed to execute this Act by the minister.

"Secretary" means Secretary of the Office of the National Cybersecurity Committee.

"Office" means the Office of the National Cybersecurity Committee.

Section 4 the Prime Minister shall have charge and control of the execution of this Act.

Chapter I
National Cybersecurity

Section 5 The maintenance of national Cybersecurity must operate to protect, tackle, prevent and reduce risks arising from circumstances of cyber threats which affect both internal and external national security covering economic stability, domestic peace and order, and which may affect military security or significantly affects the country's overall Cyber security, in a uniform manner. In doing so, consideration must be made as regards the coherence with the National Security Council's policy framework and master plan concerning the maintenance of security as approved by the Council of Ministers.

The operation for the maintenance of Cybersecurity therefore must at least cover the following areas:

(1) Integration of the country's Cybersecurity management;
(2) Capacity building for the purpose of responding to Cybersecurity emergencies;
(3) Safeguard of the country's important information infrastructure;
(4) Alignment of co-operation between the public and private sectors on Cybersecurity;
(5) Raising awareness of and knowledge on Cybersecurity;
(6) Development of regulations and legislations on Cybersecurity;
(7) Research and development on Cybersecurity;
(8) Alignment of international co-operation on Cybersecurity.

Chapter II
The National Cybersecurity Committee

Section 6 There shall be a committee called "The National Cybersecurity Committee" (NCSC) consisting of:

(1) Minister of Digital Economy and Society as Chairperson;
(2) Secretary of the National Security Council, Permanent Secretary of the Ministry of Digital Economy and Society, Permanent Secretary of the Ministry of Defence, Commander of the Technological Crime Suppression Division, the Royal Thai Police as 4 *ex officio* members;
(3) Not more than 7 qualified members appointed by the Council of Ministers from persons having distinguished knowledge, expertise and experience in the fields of information security, information technology and communications, law, or other fields that are relevant and useful for the maintenance of Cybersecurity;

The Secretary shall *ex officio* be member and secretary, and assistant secretary shall be appointed as deemed necessary.

The selection of the qualified members in paragraph 1 shall comply with the Procedures specified by the Council of Ministers and published in the Government Gazette.

Section 7 The NCSC shall have the following powers and duties:

(1) to determine the approaches and measures for responding to and tackling cyber threats in the event of undesirable or unforeseeable situation or circumstance concerning security that affects or may cause significant or serious impact, loss or damage so that the NCSC becomes the centre of operation in the event of situation or circumstance concerning security in a timely and uniform manner, unless the cyber threat is such that affects military security, which is a matter within the powers of Defence Council or the National Security Council;

(2) to determine the operation procedures for the co-operation and facilitation of operations with committees set up under other legislations, State agencies or private agencies in the order to efficiently and swiftly solve the issues of cyber threat;
(3) to determine the measures and approaches to improve the high-level skills and expertise of the Officials appointed under this Act;
(4) to make operation plans on national Cybersecurity that are coherent with the policies, strategies and National Plans on the Development of Digital Economy and Society, and the National Security Council's policy framework and master plan concerning the maintenance of national security;
(5) to make reports summarising the results of operations that result in significant impact and report these to the National Security Council and the Council of Ministers respectively;
(6) to make recommendations and give opinions to the Digital Economy and Society Commission or the Council of Ministers on the process of considering approvals for plans, projects, operations of State agencies, and on the process of considering solutions for issues or obstacles, which include legislating or amending the laws concerning the maintenance of Cybersecurity, in order to ensure the stability and sustainability of the protection, tackling, prevention and reduction of risks arising from circumstances concerning cyber threats which affect both internal and external national security;
(7) to appoint sub-committees or working groups in order to consider matters or act as entrusted by the Committee;
(8) to order or co-operate with State agencies or private agencies in order to comply with policies or operation plans concerning the maintenance of Cybersecurity or perform other acts that are necessary for the maintenance of both domestic and international Cybersecurity;
(9) to monitor and assess the execution of this Act;
(10) to perform other acts concerning the maintenance of Cybersecurity as entrusted by the Digital Economy and Society Commission.

Section 8 Qualified members shall have qualifications and not be under the prohibitions, as follows:
(1) being of Thai nationality;
(2) being bankrupt or having been dishonestly bankrupt;
(3) being incompetent or quasi-incompetent;
(4) having been sentenced by a final judgment to imprisonment notwithstanding the suspension of the sentence, except for an offence committed through negligence or a petty offence;
(5) having been expelled, dismissed or removed from the official service, a State agency, a State enterprise, or a private agency on the grounds of dishonest performance of duties or gross misconduct.

Section 9 Qualified members shall hold office for a term of 3 years.

In the case where a qualified member vacates the office before term, the Council of Ministers may appoint another person to replace him/her and that person shall remain in office for remaining term of the qualified member, except where the remaining term of the qualified member is less than 90 days, the appointment of a new qualified member may not have to be made.

Upon the expiration of term under paragraph 1, if a new qualified member has not yet been appointed, qualified members who vacate office shall remain in office to continue their duties until the new qualified members have been appointed.

A qualified member who vacates office upon the expiration of term may be reappointed, but may not be appointed for more than 2 consecutive terms.

Section 10 In addition to vacating office upon the expiration of term under Section 8, a qualified member appointed by the Council of Ministers vacates office upon:

(1) death;
(2) resignation;
(3) being dismissed by the Council of Ministers due to disgraceful behaviour, negligence or dishonesty in the performance of duty, or inefficiency;
(4) being disqualified or under any of the prohibitions under Section 7.

Section 11 Meetings, voting, and the operation of the NCSC, sub-committees and working groups shall comply with the Rules specified by the Committee.

In the performance of duty, the NCSC may entrust one or more members to perform in place of the NCSC, but the NCSC may not rely on this fact to relieve itself of responsibility.

Section 12 The NCSC shall have the power to appoint consultants for the purpose of conducting studies, make recommendations, or perform any act as entrusted by the NCSC.

The number of consultants appointed under paragraph 1 shall not exceed 5.

Section 13 The NCSC shall receive meeting allowance and other benefits as specified by the Rules issued by the Council of Ministers.

The sub-committees, working groups and consultants appointed by the NCSC shall receive meeting allowance and other benefits as specified by the Procedures issued by the NCSC.

Chapter III
Office of the National Cybersecurity Committee

Section 14 The Office of the National Cybersecurity Committee shall be set up as a State agency having a juristic person, not being a State division or a State enterprise.

Section 15 The Office shall have its headquarter located in Bangkok or a nearby province.

Section 16 The activities of the Office shall not fall within the scope of application of the law on labour protection, the law on labour relations, the law on social security and the law on compensation, but Officials and employees of the Office shall receive remunerations and benefits not less than those specified by the law on labour protection, the law on social security and the law on compensation.

Section 17 The Office shall have the following powers and duties:

(1) to respond to and tackle cyber threats in the event of undesirable or unforeseeable situation or circumstance concerning security that affects or may cause significant or serious impact, loss or damage by issuing operation measures that take into account the degree of secrecy and the access to classified information;

(2) to co-operate on operations with State agencies or private agencies in order to efficiently and swiftly solve the issues of cyber threat;

(3) to co-operate with State agencies or private agencies for the purpose of collecting information on cyber threats, the prevention and tackling of circumstances of cyber threat, and other information concerning the maintenance of Cybersecurity, to be analysed and submitted to the NCSC for consideration;

(4) to manage overall plans and co-operate on the management and the execution of the operation plans or orders of the NCSC;

(5) to monitor and speed up the operations of the State agencies involved in maintaining Cybersecurity, and report to the NCSC;

(6) to act as the centre for the information network on the country's internal and external Cybersecurity;

(7) to monitor, keep under surveillance and raise awareness on threats to the information system, including setting up and managing the Nation Computer Emergency Response Team (National CERT);

(8) to conduct studies and research on the information necessary for the maintenance of Cybersecurity for the purpose of making recommendations on measures on Cybersecurity;

(9) to encourage, support and carry out the dissemination of knowledge and the provision of services concerning the maintenance of Cybersecurity, along with holding training seminars aimed at improving skills concerning the standard of Cybersecurity or any other issue concerning Cybersecurity;

(10) to report on the progress and circumstances concerning the execution of these Rules, including issues and obstacles to the NCSC;

(11) to be in charge of administrative tasks, academic tasks, meetings, and secretarial tasks of the NCSC;

(12) to make annual reports summarising the operation and submit to the NCSC, except in case of emergency where the NCSC must be informed immediately;

(13) to perform other acts concerning national Cybersecurity as entrusted by the NCSC or the Council of Ministers.

Once the Council of Ministers approves the operation plan on national Cybersecurity under (1), the Office shall co-operate with the State agencies involved in order to carry out such plan.

Section 18 For the purpose of the fulfilment of the objectives under Section 17, the Office shall have the following powers and duties:

(1) to acquire ownership, possessory right and other proprietary rights;

(2) to create a right or enter into all kinds of legal transactions binding on a property, including other legal transactions for the benefit of the Office's carrying out of its activities;

(3) to enter into an agreement and co-operate with other organisations or agencies, both in the public and the private sectors, in activities concerning the fulfilment of the Office's objectives;

(4) to perform other necessary or continuous acts for the purpose of fulfilling the Office's objectives.

Section 19 The funds and assets for the Office's operation consist of:

(1) Money and assets transferred under Section 34;

(2) General subsidies as appropriately allocated by the Government;

(3) Subsidies from the private sector, local authorities, or other agencies including foreign sources or international organisations, and money or assets from donation;

(4) Interests or income from the assets of the Office.

The manner in which money or assets is/are obtained under (3) shall not deprive the Office of its autonomy or impartiality.

Section 20 All income received by the Office shall belong to the Office for the purpose of paying expenses incurred in the operation of the Office and shall not be included in the State's income.

Section 21 There shall be a Secretary who is directly accountable to the Chairperson of the NCSC as regards the operation of the Office and supervises the Officials and employees of the Office.

As regards activities dealing with third parties, the Secretary shall represent the Office. The Secretary may entrust any person to perform any specific act in his place in accordance with the Rules issued by the Committee and published in the Government Gazette.

The Committee shall have the power to select, appoint and remove the Secretary.

Section 22 A candidate for the position of the Secretary shall have the qualifications as follows:

(1) being of Thai nationality;

(2) being not more than 65 years of age;

(3) being able to work for the Office full-time.

Section 23 A person having any of the following prohibitions shall not take the position of the Secretary:

(1) being bankrupt or having been dishonestly bankrupt;

(2) being incompetent or quasi-incompetent;

(3) having been sentenced by a final judgment to imprisonment notwithstanding the suspension of the sentence, except for an offence committed through negligence or a petty offence;

(4) being a civil servant, official or employee of a State division or a State enterprise or another State agency or a local authority;

(5) being or having been a political official, a person holding political position, a member of local assembly or local administrator, except where such person vacates office for not less than 1 year;

(6) being or having been a director or a person holding any other position in a political party or an official of a political party, except where such person vacates office for not less than 1 year;

(7) having been expelled, dismissed or removed from the official service, a State agency, a State enterprise, or a private agency on the grounds of dishonest performance of duty or gross misconduct.

Section 24 The Committee shall determine the rate of salary and other benefits of the Secretary.

Section 25 The Secretary shall hold office for a term of 4 years.

The Secretary who vacates office upon the expiration of term may be reappointed, but may not be appointed for more than 2 consecutive terms.

Section 26 In addition to vacating office upon the expiration of term, the Secretary vacates office upon:

(1) death;

(2) resignation;

(3) being disqualified under Section 22 or being under any of the prohibitions under Section 23;

(4) being removed by a resolution of the Committee due to negligence or dishonesty in the performance of duty, disgraceful behaviour or inefficiency.

Chapter IV
Operation and Tackling of Cyber Threats

Section 27 Once the NCSC produces the Master Plan on National Cybersecurity, the Office shall produce approaches, measures, operation plans, or projects on the maintenance of Cybersecurity that are coherent and consistent with such policy and master plan.

Once the Committee approves the approaches, measures, operation plans, or project(s) on the maintenance of Cybersecurity and these come into effect, the NCSC is, in case of necessity, shall have the power to amend or supplement these as appropriate.

Section 28 The performance, by State agencies, of acts within their powers and duties under the law(s) applicable to them shall be coherent with the approaches, measures, operation plans, or projects under Section 27. Such performance is deemed to be the execution of that which is required by the Council of Ministers.

The head of State agencies shall have the duty of ensuring that the performance under paragraph 1 is carried out smoothly and achieves its goals in the specified timeframe.

In case where the NCSC monitors the progress and assesses the performance, including where it performs any act, State agencies shall have the duty of assisting and facilitating such performance of duty.

Section 29 In case where it is deemed appropriate, the NCSC may require State agencies to submit a list of persons responsible as regards the approaches, measures, operation plans, or projects on the maintenance of Cybersecurity or of persons responsible in the localities, to the NCSC for the purpose of appointment of person(s) responsible for the operation of preventing and solving issues of cyber threat.

The person(s) appointed under paragraph 1 shall perform the operation by adhering to the operation plans, resolutions, or commands of the NCSC or the orders of the Chairperson of the NCSC or of any person entrusted by the Chairperson with the approval of the NCSC.

Non-performance of paragraph 2 is deemed to be insubordination to the supervising official.

Section 30 The Prime Minister shall be in command with powers to control and direct the maintenance of Cybersecurity across the country in accordance with the operation plans on the maintenance of Cybersecurity and this Act. For this purpose, the Prime Minister shall have the power to command and order the persons responsible for the operation under Section 28 across the country.

Section 31 In case where the NCSC issues a resolution holding that a ministry, State agency or any person in charge of executing this Act fails to execute this Act or operates in contravention of an approach issued under this Act, the NCSC shall advise the ministry, State agency, or the person so in charge to correct, cancel or terminate such act within a specified timeframe. In case where the ministry, State agency or the person so in charge fails to comply with the resolution of the NCSC within the specified timeframe without reasonable excuse, the Permanent Secretary of the ministry, the head of the State agency or the person so in charge, depending on the circumstances, shall be deemed to have committed a disciplinary breach and the matter shall be submitted to the relevant authority for the purpose of disciplinary proceedings.

In case where a consequence of the failure to comply with the resolution of the NCSC under paragraph 1 causes serious damage to the civil service, such persons shall

be deemed to have wrongfully performed their duty or have committed a gross disciplinary breach, depending on the circumstances.

In case where the person failing to comply with the resolution of the NCSC under paragraph 1 is a minister, the NCSC shall report to the Prime Ministry for his/her consideration for action as he/she sees fit.

Section 32 In case where a incident of cyber threat occurs or is expected to occur in the information system under the supervision of any State agency, that State agency or the person in charge of the operation under Section 28 shall promptly report such incident to the Secretary.

Once the Secretary is informed of such incident under paragraph 1, he/she shall immediately take appropriate action to prevent or solve such cyber threat and report to the NCSC for its consideration for action.

Section 33 Upon the occurrence of an emergency or danger as a result of cyber threat that may affect national security, the NCSC shall have the power to order all State agencies to perform any act to prevent, solve the issues or mitigate the damage that has arisen or that may arise as it sees fit and may order a State agency or any person, including a person who has suffered from the danger or may suffer from such danger or damage, to act or co-operate in an act that will result in timely control, suspension, or mitigation of such danger and damage that have arisen.

In case where a person is known to be involved in the causing of the cyber threat, the NCSC shall have the power to prohibit such person from acting in any way that will result in aggravating the violence resulting from the cyber threat.

Section 34 In case where it is necessary, for the purpose of maintaining Cybersecurity, which may affect financial and commercial stability or national security, the NCSC may order a private sector to act or not to act in any way and to report the outcome of the order to the NCSC as required by the Notification of the NCSC.

Chapter V
Officials

Section 35 For the purpose of performing their duties under this Act, the Officials who have been entrusted in writing by the Secretary shall have the following powers:

(1) to issue letters asking questions or requesting a State agency or any person to give testimony, submit an explanation in writing, or submit any account, document, or evidence for the purpose of inspection or obtaining information for the benefit of the execution of this Act;

(2) to issue letters requesting State agencies or private agencies to act for the benefit of the NCSC's performance of duty;

(3) to gain access to information on communications, either by post, telegram, telephone, fax, computer, any tool or instrument for electronic media communication or

telecommunications, for the benefit of the operation for the maintenance of Cybersecurity.

The performance under (3) shall be as specified by the Rules issued by the Council of Ministers.

Section 36 Officials are prohibited from disclosing or passing on the information obtained under Section 35 to any person.

Paragraph 1 shall not apply to cases where such acts are done for the purpose of prosecuting offenders under this Act or for the purpose of prosecuting Officials involved in abuse of powers or where such acts are ordered or authorised by the Court.

Any Official who violates paragraph 1 shall be liable to imprisonment for a term not exceeding 3 years, or to a fine not more than 60,000 baht, or to both.

Section 37 The appointment of Officials under this Act shall be done by the Prime Minister, from persons having expertise on computer system or information security and having qualifications as specified by the minister.

Section 38 For the benefit of the co-operation or operation, officials of the Ministry of Defence who have been entrusted with a mission to respond to or tackle cyber threats that affect military security shall be Officials under this Act.

Section 39 In the performance of duty under this Act, Officials shall be officials under the Criminal Code.

In the performance of duty under this Act, Officials shall display their identity card to the persons involved. The identity card shall be in the form published by the minister in the Government Gazette.

Chapter VI
Transitional Provisions

Section 40 All activities, powers and duties, funds and assets of the Security Bureau, Electronic Transactions Development Agency existing on the date of coming into force of this Act shall be transferred to the Office under this Act.

Section 41 Officials and employees of the Electronic Transactions Development Agency under Section 42 who perform duties on the date of coming into force of this Act, if willing to be transferred and become Officials or employees of the Office, shall express such intention in writing to their supervising official within 30 days of the date of coming into force of this Act. Those who do not express such intention within such timeframe shall return to perform duties at the Electronic Transactions Development Agency.

The recruitment and appointment of Officials and employees under paragraph 1 to any position in the Office shall be in accordance with the capacity, qualifications and rate of salary or wage as specified by the Committee, but these shall not be less than their previous salary or wage.

Section 42 The Electronic Transactions Development Agency shall perform the duties of the Office of the National Cybersecurity Committee until such time that the Office is set up in accordance with this Act.

Section 43 Once this Act comes into force, during the initial period, the committee shall consist of the Minister of Digital Economy and Society as Chairperson; the Permanent Secretary of the Ministry of Digital Economy and Society as Vice-Chairperson; the Secretary of the National Security Council, the Commander of the Technological Crime Suppression Division, the Royal Thai Police as members; and the Director of the Electronic Transactions Development Agency as member and secretary.

The committee under paragraph 1 shall temporarily perform the duties of the Committee until such time that the Committee under this Act is set up, the timeframe for which shall not exceed 90 days from the date of coming into force of this Act.

Countersigned by:

…….

Prime Minister