LAW OF MONGOLIA ON CYBER SECURITY

17 December 2021 **State Palace, City of Ulaanbaatar**

CHAPTER ONE

GENERAL PROVISIONS

Article 1. Purpose of the law

1.1. The purpose of this law is to regulate relations pertaining to establishing the system, principles, and legal framework in ensuring cyber security, and ensuring the safety, confidentiality, and accessibility of information within cyberspace and cyber environments.

Article 2. Legislation on cyber security

2.1. Cyber security legislation shall consist of the Constitution of Mongolia, Law on National Security, Law on Armed Forces, Law on State and Official Secrets, Law on Communications, Law on the Intelligence Agency, Law on Organizational Secrets, Law on Transparency of Public Information, Law on Personal Secrets, the Law on Electronic Signatures, this law, and other legislative acts enacted in accordance thereto.

2.2. Where an international treaty to which Mongolia is party stipulates differently from this law, the rules of such international treaty shall prevail.

Article 3. Scope of application of the law

3.1.This law applies to relations of coordinating, facilitating, and monitoring relations between the State, inpiduals, and legal persons in ensuring cyber security.

3.2. Unless otherwise stipulated in the law, this law shall apply indiscriminately to foreign citizens, stateless persons, and foreign or foreign-invested legal persons operating through the information systems and information networks of Mongolia.

3.3.The auditing of information security regulated by this law shall not comprise auditing by state audit organizations.

Article 4.Definition of terms in this law

4.1.The following terms used in this law shall have the following definitions, respectively:

4.1.1."cyber security" shall mean the fulfillment of safety, confidentiality, and accessibility of information within cyber environments;

4.1.2."cyberspace" shall mean tangible and non-tangible platforms that consist of internet and other information and communication networks, and inter-dependent systems that ensure their operation;

4.1.3."cyber environment" shall mean the information systems, and information network environments that allow accessing, login, collection, processing, storing, and use of information;

4.1.4."safety" shall mean protection from unauthorized deletion or modification;

4.1.5."confidentiality" shall mean the state of protection of information from unauthorized access or login;

4.1.6."accessibility" shall mean the possibility of accessing, logging in, collecting, and using of information within the allowed scope;

4.1.7."information system" shall have the meaning as stipulated in article 4.1.1 of the Law on Transparency of Public Information;

4.1.8."information network" shall have the meaning as stipulated in article 4.1.2 of the Law on Transparency of Public Information;

4.1.9."cyber security risk assessment" shall have the meaning professional activities that define the probability of failure of, threats and risks to, the cyber security of electronic information, information systems, and information networks, the level of vulnerability, and measures to reduce its consequences and risks, and of prevention;

4.1.10."information security audit" shall mean unbiased, independent professional activities that review the compliance with cyber security laws and relevant procedures and standards and issue recommendations;

4.1.11."log of information system actions" shall mean the registration that defines the action and time of access, login, processing, collecting, and use to a specific information system;

4.1.12."Organization with critical information infrastructure" shall mean an organization that has an information system or information network, of which the failure of the cyber security could potentially cause failure of such organization's operations, and cause harm to the security, society, and economy of Mongolia;

4.1.13."Cyber security violation" shall mean any act or omission thereof that threatens the safety, confidentiality, or accessibility of an information system;

4.1.14."cyber-attack" shall mean an action that aims to disrupt the cyber security of information systems or information networks;

4.1.15."cyber-attack at national level" shall mean a cyber-attack that attacks the information system and information network of an organization with critical information infrastructure thereby disrupting the operations of such organization potentially causes harm to the national security, society, and economy of Mongolia;

4.1.16."Center against cyber-attacks and violations" shall mean person charged with the function to facilitate activities to prevent, detect, terminate, and respond to cyber-attacks and violations, and restore information systems, and provide professional guidance thereto;

4.1.17."State information consolidated network" shall mean the comprehensive system of state internet usage and official and special use networks, with a consolidated infrastructure aimed at ensuring information-exchange and cyber security between state organizations;

4.1.18."state-owned legal person" shall have the meaning stipulated in article 13 of the Law on State and Local Properties.

Article 5.Principles of ensuring cyber security

5.1.In addition to that stipulated in article 4.1 of the Law on National Security, the following principles shall be adhered to in ensuring cyber security:

5.1.1.maintain unified supervision;

5.1.2.to be grounded on science, progressive technology and innovation;

5.1.3.support national products, services, and human resources capabilities;

5.1.4.to base on risk assessment;

5.1.5.to base on public-private partnership;

5.1.6.develop international cooperation.

CHAPTER TWO
ACTIVITIES TO ENSURE CYBER SECURITY

Article 6.Workstreams in ensuring cyber security

6.1.The work of ensuring cyber security shall consist of the following workstreams:

6.1.1.policy, administration, facilitation;

6.1.2.technical and technological measures to ensure cyber security;

6.1.3.prevention from, and promoting awareness of cyber-attacks and violations;

6.1.4.detection, termination of, and responding to cyber-attacks and violations, restorative measures..

Article 7.Common procedures to ensure cyber security

7.1.The Government shall adopt the common procedures on ensuring cyber security, prevention, detection and counter-responses.

7.2.The legal persons stipulated in articles 16.1, 17.1, and 19.1 of this law shall have its internal procedure in ensuring cyber security that conforms to the common procedure to ensure cyber security.

Article 8.Cyber security risk assessment

8.1.Cyber security risk assessment shall be conducted by legal persons registered at the state central administrative organization in charge of digital development and communications.

8.2.The legal person stipulated in article 8.1 of this law shall have an employee on staff that has been certified by an international professional or standards association, or an equivalent organization.

8.3.The state central administrative organization in charge of digital development and communications and the intelligence agency shall jointly adopt the procedures and methodology for conducting cyber security risk assessment.

8.4.The intelligence agency, or by the permission thereof a legal person stipulated in article 8.1 of this law shall conduct the cyber security risk assessment of organizations connected to the state information consolidated network, and of state-owned legal persons with critical information infrastructure.

8.5.The legal persons stipulated in article 8.1 of this law, and the relevant organization and official who have received the cyber security risk assessment report shall be obligated to maintain the confidentiality and ensure non-disclosure thereof.

Article 9.Information security audit

9.1.Information security audits shall be conducted by legal persons registered with the state central administrative organization in charge of digital development and communications.

9.2.The following requirements shall be met by legal persons to conduct information security audits:

9.2.1. Have an employee on staff that has been certified by an international professional or standards association, or an equivalent organization to conduct information security audits;

9.2.2.The employee stipulated in article 9.2.1 of this law shall not maintain simultaneous employment with other legal person authorized to conduct audits of the same type;

9.2.3.Other requirements stipulated in the law.

9.3.It shall be prohibited for a legal person conducting information security audit to conduct

information security audits on the same organization two years after such time that it has rendered information technology and information security services to such organization.

9.4.Organizations with critical information infrastructure shall have its information security audits conducted by the intelligence agency, or with the permission thereof, by legal person stipulated in article 9.1 of this law.

9.5.The state central administrative organization in charge of digital development and communications shall adopt procedures on registering legal persons to conduct information security audits, and on conducting audits.

9.6. The legal persons stipulated in article 9.1 of this law, and the relevant organization and official who have received the information security audit report shall be obligated to maintain the confidentiality and ensure non-disclosure thereof.

CHAPTER THREE
CYBER SECURITY SYSTEM

Article 10. Government

10.1.In accordance with the national security framework, the Government shall implement the following authority regarding ensuring cyber security:

10.1.1.adopt the national strategy on cyber security;

10.1.2.incorporate cyber security within development policy and planning documents, facilitate the implementation of legislation accordingly;

10.1.3.adopt a national level plan for protection from cyber-attacks;

10.1.4.adopt the rules, organizational structure, staff positions of the national center against cyber-attacks and violations and the public center, the operational procedure of the centers, and their operational requirements;

10.1.5.adopt the list of organizations with critical information infrastructure;

10.1.6.adopt the procedure for establishing and using the state information consolidated network, and the list of organizations affiliated thereto;

10.1.7.incorporate funds necessary for implementing activities aimed at ensuring cyber security, within the state budget;

10.1.8.adopt the organizational structure, staff positions, and operational procedure of the cyber security council office.

Article 11.Cyber Security council

11.1.A non-staff Cyber security council (hereinafter referred to as "the Council") shall operate with the key functions to provide cyber security activities with unified supervision, coordinated facilitation, organize implementation, and ensure exchange of information.

11.2.The Council shall be led by the Prime Minister, and the vice-director shall be the Member of Government in charge of digital development and communications as well as the Head of the General Intelligence Agency, and the Council shall have an office.

11.3.The constitution and the rules of the Council shall be adopted by the Government.

11.4.The Council shall implement the following authority:

11.4.1.Exercise monitoring on the implementation of the cyber security legislation;

11.4.2.provide unified supervision and facilitation on ensuring cyber security at the

national level, facilitate and coordinate the activities of the relevant organizations;

11.4.3.requisition from relevant organizations information and documents necessary for ensuring cyber security;

11.4.4.cooperate with foreign countries and international counterpart organizations on ensuring cyber security;

11.4.5.other authorities stipulated in the law.

11.5.Funds necessary for the operation of the Council and its Office shall be financed by the state budget.

11.6.Decisions of the Council shall be in the form of resolutions and minutes, and seals, stamps, and letterheads made in accordance with the relevant procedures shall be used.

11.7.Council decisions issued in relation to ensuring cyber security shall be implemented by the relevant organizations and officials, and reported accordingly.

Article 12.State central administrative agency in charge of digital development and communications

12.1.The state central administrative agency in charge of digital development and communications shall exercise the following authority in relation to ensuring cyber security:

12.1.1.implement legislation and decisions of the relevant authority in relation to ensuring cyber security;

12.1.2.develop a cyber security development policy, organize its implementation;

12.1.3.develop common procedures to ensure cyber security in collaboration with the intelligence agency and the cyber security organization of the armed forces;

12.1.4.collaborate with international organizations and organizations of foreign countries in areas of cyber security;

12.1.5.develop the list of organizations with critical information infrastructure, in collaboration with the intelligence agency and the cyber security organization of the armed forces;

12.1.6.register legal person authorized to conduct cyber security risk assessments, and conduct information security audits;

12.1.7.conduct new technical, technological, innovation, research and development activities in areas of cyber security;

12.1.8.implement measures to prevent cyber-attacks and violations, to promote awareness, and advertise relevant legislation.

Article 13.Intelligence agency

13.1.The intelligence agency shall exercise the following authority in relation to ensuring cyber security:

13.1.1.organize the state information consolidated network, and ensure its cyber security;

13.1.2.exercise monitoring over activities to ensure the cyber security of organization that are connected to the state information consolidated networks, and state-owned organizations with critical information infrastructures, and organize trainings for relevant persons;

13.1.3.develop the national strategy for cyber security in collaboration with the state

central administrative organization in charge of digital development and communications, and the cyber security organization of the armed forces;

13.1.4.develop the plan for protection from national level cyber-attacks, monitor its implementation;

13.1.5.adopt jointly with the relevant organization, the procedure pertaining to information exchange with the organization specially charged to ensure national security and with state central administrative organizations;

13.1.6.develop the procedure stipulated in article 10.1.6 of this law, and monitor its implementation;

13.1.7.verify, certify, and issue conclusions on the technology and software designated to ensure the security of the information systems and information networks of the person stipulated in article 13.1.2 of this law;

13.1.8.issue conclusion to the persons stipulated in article 13.1.2 of this law in relation to the ensuring of cyber security of information technology projects and program that are to be implemented based on loans, aid, and investment from foreign countries, and submit recommendations and requirements to the relevant authorities in relation thereto;

13.1.9.operate a quantitative analysis laboratory for the purpose of fighting against cyber-attacks and violations;

13.1.10.issue its recommendation in relation to registration of persons to conduct cyber security risk assessment;

13.1.11.submit recommendations and requirements to inpiduals and legal persons in relation to ensuring cyber security.

Article 14.Cyber security organization of the armed forces

14.1.The cyber security organization of the armed forces shall exercise the following authority in ensuring cyber security:

14.1.1.organize the implementation of cyber security legislation in the defense sector;

14.1.2.in times of peace ensure cyber security and the security of defense information systems and information networks, and where necessary provide support in the activities of ensuring cyber security of the nation;

14.1.3.unless otherwise stipulated in the law, verify and certify the equipment and software of the information systems and information networks used in the defense command units and organizations;

14.1.4.organize trainings for defense command units and organizations on ensuring cyber security, and submit recommendations related thereto;

14.1.5. exchange information, and collaborate cooperate with foreign and domestic organizations of the same function in the area of ensuring cyber security capacity and readiness.

Article 15.Police authority

15.1.The police authority shall exercise the following authority in relation to ensuring cyber security:

15.1.1.Receive information on crimes related to cyber-attacks and violations, and conduct operations stipulated in the law;

15.1.2.requisition and access information necessary to implement its function stipulated

in article 15.1.1 of this law from relevant state organizations, officials, inpiduals, and legal persons;

15.1.3.submit recommendations, requirements, and warnings related to ensuring cyber security to inpiduals and legal persons;

15.1.4.operate a quantitative analytical laboratory for the purposes of fighting against cyber-attacks and violations, verify equipment and software, conduct research and development work, and issue conclusions.

Article 16.State-owned legal person

16.1.State-owned legal persons shall have the following obligations in relation to ensuring cyber security:

16.1.1.adopt internal operational procedures on ensuring cyber security;

16.1.2.comply with recommendations and requirements issued by relevant authorities on ensuring cyber security;

16.1.3.in cases of harm or potential harm from cyber-attacks and violations, immediately notify the center against cyber-attacks and violations;

16.1.4.incorporate the funds and operational expenses necessary for ensuring cyber security into the budget annually;

16.1.5.store information system action log for the time period stipulated in the common procedure for ensuring cyber security.

Article 17.Legal person

17.1.Legal persons providing information technology services in the processing, storing, distributing, computer analytics, and ensuring the normal operations through shared information systems within the cyber space, shall have the following obligations:

17.1.1.adopt internal procedures to ensure cyber security;

17.1.2. immediately notify the center against cyber-attacks and violations of cyber-attacks, obtain assistance if unable to terminate such attacks;

17.1.3. store information system action log for the time period stipulated in the common procedure for ensuring cyber security;

17.1.4.obtain professional and methodology assistance from relevant state organization, and collaborate therewith in ensuring cyber security;

17.1.5.havean officer or unit on staff in charged with ensuring cyber security;

17.1.6.have cyber security risk assessments conducted every two years, and where the circumstances stipulated in the relevant procedures have arisen have such assessments done immediately for each case, and take measures in accordance with the conclusion, recommendations, and requirements issued in relation thereto;

17.1.7. have information security audits conducted every year, and where the circumstances stipulated in the relevant procedures have arisen have such audits done immediately for each case, and take measures in accordance with the conclusion, recommendations, and requirements issued in relation thereto;

17.1.8.have the relevant cyber security verification and check-ups each time new information technology products, services, and their updates and modifications are introduced;

17.1.9.notify users immediately of cyber-attacks and violations.

17.2.If information security audits have been conducted in the time period stipulated in this law and in accordance with international standards, such audits shall be based on to deem the obligation stipulated in article 17.1.7 of this law as fulfilled.

17.3.Legal persons other than that stipulated in article 17.1 of this law shall exercise the following rights and obligations:

17.3.1.abide by the common procedures on ensuring cyber security in its activities;

17.3.2.notify the relevant center against cyber-attacks and violations of cyber-attacks and violations, and obtain assistance where necessary;

17.3.3.comply with recommendations and requirements issued by the relevant organizations;

17.3.4.other rights and obligations stipulated by legislation.

Article 18.Citizen

18.1.Citizens shall have the following obligations in ensuring cyber security:

18.1.1.take responsibility for the cyber security of themselves and any inpiduals under their care;

18.1.2.comply with and abide by the recommendations issued by the relevant organization;

18.1.3.others stipulated in legislation.

18.2.In case of potential cyber-attacks or violations, citizens may immediately notify the Public center.

Article 19.Organizations with critical information infrastructure

19.1.Organizations with critical information infrastructure shall include organizations of the following nature of business:

19.1.1.organizations with electricity production, distribution, transmission, and monitoring control systems;

19.1.2.organizations with clean and waste water, heating source, centralized grid, and distribution and monitoring control systems;

19.1.3.tier two and three health organizations;

19.1.4.laboratories for research on highly contagious or infectious diseases of humans and livestock;

19.1.5.producers of medicine, and toxic and hazardous chemicals;

19.1.6.banks and financial institutions with consolidated digital systems for payment, settlement, and transactions;

19.1.7.operators in communications, and information technology that are natural monopolies or exercise a dominant position;

19.1.8.organizations with air, railway, waterway, and auto-road transportation coordination and control systems;

19.1.9.organizations that import, producers, and distributors of fuel;

19.1.10.organizations that produce, store, and distribute strategic food stuff;

19.1.11.Information and operational management center;

19.1.12.National public radio and television;

19.1.13.organization in charge of main and supporting information systems and base information databases;

19.1.14.organization in charge of data centers, their branches and resource center operations;

19.1.15.organization in charge of border port control and administration systems;

19.1.16.organization mining minerals of strategic significance;

19.1.17.organization in charge of registration, monitoring, and consolidated information systems relating to passengers and transportation vehicles that are crossing the national borders.

19.2.Organizations with critical information infrastructure shall have the following obligations:

19.2.1.adopt internal procedures for ensuring cyber security;

19.2.2.adopt and implement an action plan in case of cyber-attacks and violations;

19.2.3.introduce standards to ensure information security;

19.2.4. have an officer or unit on staff in charged with ensuring cyber security;

19.2.5. have cyber security risk assessments conducted every year, and where modifications are made to the information systems and information networks have such assessments done partially for each case, and fully if required by the relevant authorities, and take measures in accordance with the conclusion, recommendations, and requirements issued in relation thereto;

19.2.6.have information security audits conducted every two years;

19.2.7.plan and implement management, organizational, and technical measures necessary for ensuring the information system and information network security;

19.2.8.have an information system for the detection, registration, and termination of cyber-attacks and violations;

19.2.9. store information system action log for the time period stipulated in the common procedure for ensuring cyber security;

19.2.10.submit the cyber security risk assessment and information security audit reports to the relevant center against cyber-attacks and violations within one month of receipt;

19.2.11.comply with the requirements issued by the relevant authorities, and take measures to eliminate the violations and errors detected;

19.2.12.If cyber security risk assessments are to be conducted by foreign citizens and foreign legal persons, the intelligence agency shall be consulted;

19.2.13.have an action plan in place for ensuring the normal, uninterrupted operation of the information system and infrastructure, and for restoration thereof in case of damages and interruptions;

19.2.14. notify the relevant center against cyber-attacks and violations immediately of failure of normal, uninterrupted operations of the information systems and infrastructure due to cyber-attacks and violations;

19.2.15. notify the relevant center against cyber-attacks and violations, and the users immediately of failure of normal, uninterrupted operations infrastructure due to planned inspections and audits, damages and events and circumstances of force majeure to networks and systems outside of their own infrastructure.

19.3. If information security audits have been conducted in the time period stipulated in this law and in accordance with international standards, the report of such audit shall be based on to deem the obligation stipulated in article 19.2.6 of this law as fulfilled.

CHAPTER FOUR
COMBATING CYBER ATTACKS AND VIOLATIONS

Article 20.Center against attacks and violations

20.1.The following centers with the human resources, technical and technological capacity, and information databases shall operate with the key functions to provide professional and methodology support and assistance for the detection, termination of, and responses to. cyber-attacks and violations, and for the restoration of targeted infrastructures and information systems:

20.1.1.National center against cyber-attacks and violations (hereinafter referred to as "National center");

20.1.2.Public center against cyber-attacks and violations (hereinafter referred to as "Public center");

20.1.3.Armed forces center against cyber-attacks and violations (hereinafter referred to as "Armed forces center").

20.2.Legal persons other than the above shall have fulfilled the relevant requirements stipulated in article 10.1.4 of this law in conducting activities to detect and terminate cyber-attacks.

20.3.The centers stipulated in article 20.12 and 20.1.3 of this law, and the legal person stipulated in article 20.2 of this law shall cooperate with the National center and exchange information regarding cyber-attacks and violations.

Article 21.National Center

21.1.The National center shall fall under the structure of the intelligence agency.

21.2.The National center shall exercise the following functions:

21.2.1.coordinate and facilitate the activities and operation of the centers against cyber-attacks and violations nationwide, and provide professional and methodology assistance thereto;

21.2.2.detect, terminate, and respond to cyber-attacks and violations directed at the information systems of state-owned legal persons with critical information infrastructure and organizations connected to the state information consolidated network, and provide support in the restoration of the targeted information systems;

21.2.3.conduct analysis, accumulate databases, develop statistical information and surveys, and distribute recommendations and information pertaining to information on cyber-attacks and violations nationwide;

21.2.4.represent Mongolia in collaborations and exchange of information with international organizations and organizations of foreign countries in areas that fall under the scope of authority;

21.2.5.receive information pertaining to cyber-attacks and violations, transfer such information to the relevant authorities;

21.2.6.issue and submit recommendations and requirements regarding cyber-attacks

and violations to organizations with critical information infrastructure and other relevant organizations and officials;

21.2.7. for the purposes of categorizing, processing, information regarding cyber-attacks and violations registered nationwide, and transferring such information to the relevant authorities, operate a team consisting of representatives of relevant organizations.

Article 22.Public center

22.1.The Public center shall operate under the state central administrative organization in charge of digital development and communications.

22.2.The Public center shall exercise the following functions:

22.2.1.detect, terminat, and respond to cyber-attacks and violations directed at inpiduals and legal persons other than that stipulated in article 21.2.2 of this law, and provide support in the restoration of the targeted information systems;

22.2.2.conduct research and analysis on cyber-attacks and violations, and distribute recommendations and information thereon to the public;

22.2.3.cooperate and exchange information with the centers stipulated in article 20.1.1, and legal persons stipulated in article 20.2 of this law;

22.2.4. issue and submit recommendations and requirements regarding cyber-attacks and violations to citizens and legal persons.

Article 23.Armed forces center

23.1.The Armed forces center shall operate within the structure of the Armed forces cyber security organization.

23.2.The Armed forces center shall exercise the following functions:

23.2.1.prevent, detect, terminate, and respond to cyber-attacks and violations directed at defense sector information systems, and restore targeted information systems;

23.2.2.render support to the activities of prevention of foreign cyber-attacks and threats;

23.2.3. cooperate with foreign countries and international counterpart organizations on ensuring cyber security.

23.2.4.verify and certify and issue conclusions on the technical equipment and software designated to ensure the cyber security in the defense sector.

CHAPTER FIVE
MISCELLANEOUS

Article 24.Liabilities imposable on violators of the legislation on cyber security

24.1.If the actions of the official who has violated this law does not carry the characteristics of a crime, the liabilities stipulated in the Law on Public Service or the Labor Law.

24.2.An inpidual or legal person who has violated this law shall be imposed liabilities stipulated in the Criminal Law or the Law on Violations.

24.3.The delegation by an organization or legal person of its activities to ensure its cyber security to others on a contractual basis shall not serve as grounds for exemption from liabilities.

Article 25.Enforcement of the law

25.1.This law shall be enforced from 1 May 2022.

SPEAKER OF THE STATE GREAT KHURAL OF MONGOLIA
G. ZANDANSHATAR