Law of Georgia on Information Security

Chapter I.
General provisions

Article 1. Purpose of the Law

The purpose of this Law is to facilitate effective and efficient enforcement of information security, provide information security rights and obligations in public and private sector, and define state control mechanisms for implementation of information security policy.

Article 2. Use of terms

For the purposes of this Law, terms used herein shall have the following meaning:

a) **Information security** – activity that ensures protection of access to, unity, authenticity, confidentiality and continuous operation of information and information systems;

b) **Information security policy** –provisions, principles and practices contained in this Law, other normative acts of Georgia and international agreements, aimed at ensuring information security policy and is compliant with established international standards in this area;

c) **Cyberspace** – environment characterized by use of electronic devices and electromagnetic spectrum for storage, alteration or exchange of data by use of networked systems and supporting physical infrastructure;

d) **Cyber attack** – action that uses electronic device and/or connected network or system in order to breach integrity of systems, property or functions of an information system, as well as to obstruct, destroy or illegally obtain information from such systems, property or functions;

e) **Computer incident** – a real or potential violation of information security policy that is carried out by use of information technology and causes unauthorized access to information, information leakage, suspension of service or appropriation of information resource;

f) **Critical information system** – an information system whose uninterrupted operation is important for the defense and/or economic security of the state, as well as for normal functioning of the state and/or society;

g) **Critical information system subject** – a legal entity or state agency whose uninterrupted operation of its information systems is important for the defense and/or economic security of the state, as well as for normal functioning of the state and/or society;

h) **Confidential information** – information that, where its confidentiality, integrity or availability is breached, would potentially cause significant damage to operation of the critical information system subject. The goal of classifying information as confidential is to ensure compliance with rules of information asset management, without prejudice to provisions of the General Administrative Code of Georgia that define access to public information;

i) **Information for internal use** –information that is designated for internal use by employees or contractors of the critical information system subject, where its confidentiality, integrity or availability is breached, would potentially cause significant obstruction to operation of the critical information system subject, or would cause harm to state interest or business reputation of the private entity. The goal of classifying information for internal use is to ensure compliance with rules of information asset management, without prejudice to provisions of the General Administrative Code of Georgia that define access to public information;

j) **Information asset** – any information and knowledge that has value for critical information system subject, including technological means for storage, processing and transfer of information, as well as employees and their knowledge of information processing;

m) **Information system** – any combination of information technology and acts performed by such technology that facilitates management and/or decision-making;

n) **Network sensor** – device specifically intended for monitoring a segment of the network in order to identify acts that point to attack against or breach of information system;

o) **Data Exchange Agency** - Legal Entity of Public Law under the Ministry of Justice of Georgia (hereinafter – Data Exchange Agency);

p) **Cyber Security Bureau** – Legal Entity of Public Law under the Ministry of Defense of Georgia (hereinafter - Cyber Security Bureau).

Article 3. Scope of application

1. This Law is applicable to legal persons and state agencies recognized as critical information system subjects. This Law also extends to organization or entity that operates within competence of the critical information system subject or is in employment, internship, contract or any other relationship with the critical information system subject where such relationship provides access to information assets.

2. A specific list of critical information system subjects and their categorization as to criticality is defined by the Decree of the Government of Georgia, the draft of which shall be presented by the Ministry of Justice of Georgia in consultation with the Ministry of Defense and the Ministry of Internal Affairs. The list should be drafted according to the following criteria: potential severity and scope effects caused by downtime or destruction of an information system; potential economic impact on

the subject and the state; degree of viability of the information system for the normal functioning of the society; number of users of the system; economic state of the subject in question and cost of compliance with obligations deriving from the law.

3. This law does not apply to mass media, publishing companies, scientific, educational, religious and community organizations, as well as political parties, irrespective of the importance of their activities for the defense and/or economic security of the state, as well as for normal functioning of the state and/or society.

4. Any legal entity or state agency that is not a critical information system subject may voluntarily avail itself of obligations deriving from this Law.

5. The scope of this Law excludes actions aimed at testing information security authorized in advance by the critical information system subject.

6. Provisions of this Law are without prejudice to application of provisions of the Georgian law that govern freedom of information, personal data protection, and protection of state, commercial or private secrets.

Chapter II. Organization and enforcement of information security

Article 4. Information security policies

1. Critical information system subject shall adopt internal rules of information security that enforce provisions of this Law and define information security policy of the institution.

2. Information security policy shall be compliant with the minimum standards of information security based on criticality classification of the subject that are determined by the Data Exchange Agency and are in conformity with relevant standards and requirements set by International Standardization Organization (ISO) and Information Security Audit and Control Association (ISACA).

3. Critical information system subject shall communicate information security policy adopted in compliance with par. 1 of this Article to the Data Exchange Agency for review. The Data Exchange Agency shall be also notified of any changes to information security policies. The Data Exchange Agency conducts general analysis of submitted documents and present recommendations for remedying shortcomings identified.

4. Beyond documents directly noted in par. 3 of this Article, the Data Exchange Agency shall have no access to information or information asset of the critical information system subject, unless the latter voluntarily grants the Data Exchange Agency access to information or information asset.

Article 5. Information assets management

1. In accordance with internal rules under par. 1 of Article 4 of this Law, critical information system subject shall conduct inventory assessment (description) of all information assets resulting in assignment of a specific criticality class to each

information asset – confidential or for internal use. Any other asset that does not require such classification is considered to be open information.

2. As a result of inventory assessment of information assets, each asset shall be assessed as to importance, value, security and current level of protection.

3. At the time of creation of information asset, the corresponding criticality class is assigned by an author and/or responsible person.

4. Rules detailing inventory assessment, classification, access, publication, alteration and deletion of information assets are set by normative act adopted by the Data Exchange Agency, excluding rules that define access to public information according to the General Administrative Code.

Article 6. Information security audit and information system testing

1. Based on the consent of the critical information system subject, the Data Exchange Agency or a person or organization selected by the critical information system subject from the pool of organizations or persons duly authorized by the Data Exchange Agency, shall conduct assessment of compliance of the information security policy of the critical information system subject with minimum security standards set by the Data Exchange Agency (information security audit). Audit report created as a result of information security audit is subject to obligatory implementation.

2. Information security audit defined under par. 1 of this Article shall be conducted in accordance with rules set by the normative act adopted by the Data Exchange Agency.

3. The cost of information security audit delivered by the Data Exchange Agency is determined on a basis of a contract with the critical information system subject.

4. Data Exchange shall adopt a normative act defining rules for authorization of persons or organizations eligible to perform information security audit, as well as procedures and costs for such authorization.

5. Data Exchange Agency or an independent and duly competent person or organization selected by the critical information system subject with prior consent of the Data Exchange Agency, shall conduct penetration testing and vulnerability assessment of information systems in accordance with duly planned and documented task description.

6. In case where audit or testing identifies non-compliance, the critical information system subject shall conduct analysis of causes for non-compliance and, where necessary, defines and undertakes due remedies, the action plan of which shall be communicated to the Data Exchange Agency.

Article 7. Information Security Manager

1. Critical information system subject shall appoint a specific person(s) or an employee responsible for ensuring compliance with information security

requirements of the critical information system subject (hereinafter: Information Security Manager).

2. Main responsibilities of Information Security Manager shall include:

a) Daily monitoring of implementation of the information security policy;

b) Description of information assets and access thereto;

c) Preparation of internal information security policy documents;

d) Collecting information on information security incidents and monitoring of response;

e) Reporting on information security matters and other administrative/organizational activity;

f) Organization and conduct of general and sector-specific training in information security;

g) Other responsibilities as defined by the critical information system subject.

3. Information Security Manager is accountable to the head of the critical information system subject, or person authorized by the latter, or group of persons (collegiate body) authorized to implement information security policy. Any important decision related to implementation of information security policy shall be taken by the person(s) noted above or with the latter's prior consent.

4. Information Security Manager shall draft information security action plan and provide yearly progress report to person(s) envisaged under par. 3 of this Article and to the Data Exchange Agency.

Chapter III. Ensuring Cyber Security

Article 8. Computer Emergency Response Team

1. Computer Emergency Response Team of the Data Exchange Agency - CERT Georgia (hereinafter – CERT) shall take part in implementation of this Law, namely, by handling incidents against information security in the cyber-space of Georgia, as well as other related activity aimed at coordination of information security which aims at eliminating priority threats against cyber security.

2. Priority threats against information security include:

a) Cyber attack that threatens life and health of individuals, state interests or defense capabilities;

b) Cyber attack against information systems of the critical information system subject;

c) Cyber attack that threatens financial assets or property rights of state, private entity or an individual;

c) Any other action that, by its nature, aim, source, volume, multitude or amount of resources necessary for its suppression, contains enough danger to undermine normal operation of the critical information system.

3. CERT responsibilities shall include:

a) Providing advice on the protection of critical information system through information security;

b) Timely identification of computer incidents;

c) Providing response to computer incidents and coordination of incident response;

d) Recording computer incidents and establishing priorities and categories;

e) Computer incident analysis;

f) Providing assistance in handling consequences of computer incidents and damage reduction;

g) Coordination of measures aimed at prevention of computer incidents and assistance in implementing preventive solutions;

h) Raising awareness on information security, including information on current threats and vulnerabilities in critical information systems, unless public availability of such information is an information security threat in itself;

i) Providing wider public of computer users with alerts and relevant information on potential threats;

j) Education and dissemination on matters of information security;

k) International representation and coordination of information security matters;

l) Other functions related to objectives of information security as defined by law or other normative act.

4. CERT shall have the right to request access to information asset, information system and/or any object that is part of information infrastructure of the critical information system subject where such access is necessary for due response to ongoing or past computer incident. Information Security Manager of the critical information system subject shall, upon considering the request in reasonable time, inform CERT without delay on granting or refusing access.

5. Competences, work procedures, response mechanisms to computer incidents and other rules for CERT are defined by normative act of the Data Exchange Agency.

Article 9. Cyber security specialist

1. Critical information system subject shall appoint specific person(s) or employee(s) responsible for practical realization of computer systems security at the critical information system subject (hereinafter: cyber security specialist).

2. Main responsibilities of the cyber security specialist include:

a) Daily monitoring and assessment of computer systems;

b) Identification of and response to cyber security incidents;

c) Analysis and reporting of security incidents and measures;

d) Coordination with CERT of the Data Exchange Agency;

e) Other duties as defined by the critical information system subject.

3. Cyber security specialist is accountable to the head of information technology service of the critical information system subject or to the person duly authorized by the latter.

4. Cyber security specialist shall be available at any time of day, including hours beyond work duty, and is responsible to ensure constant coordination with the Data Exchange Agency in case of ongoing or potential cyber attack on critical information system subject, as well as in the process of handling consequences of the attack.

5. In cases where ongoing or potential cyber attack presents extraordinary threat to defense capability or economic security of the country, normal functioning of state institutions and society, Data Exchange Agency is authorized to conduct temporary coordination of cyber security specialists in order to prevent, repeal or handle consequences of such attack.

Article 10. Identification of cyber security incident

1. Critical information system subject shall identify cyber security incidents, which comprises studying, description and response to each incident.

2. Pursuant to the agreement with the critical information system subject, Data Exchange Agency and subject's cyber security specialist shall configure and manage network sensor necessary for identification and study of computer incidents in subject's network. Network sensors configuration shall be determined by the normative act of the Data Exchange Agency.

3. Identification of cyber incident shall be immediately reported to CERT and, where necessary, urgent measures undertaken in order to preserve and protect information about the incident.

4. CERT conducts study, description and proper response to cyber incidents in the course of its duties provided by this Law.

Chapter III[1]. Cyber Security Bureau

Article 10[1]. Status and functions of the Cyber Security Bureau

1. Information security policy of the defense sphere shall be compliant with the minimum standards of information security in the defense sphere (based on criticality classification of the defense sphere subjects) that are determined by the Cyber Security Bureau in conformity with relevant standards and requirements set by International Standardization Organization (ISO) and Information Security Audit and Control Association (ISACA).

2. Cyber Security Bureau is established on the basis of this Law and the Law of Georgia on Legal Entities of Pubic Law.

3. The authority of the Cyber Security Bureau does not extend to the Data Exchange Agency whose authority is determined by this Law and the Law on Legal Entity of Public Law – Data Exchange Agency.

4. A specific list of defense sphere critical information system subjects and their categorization as to criticality is defined by the Decree of the Government of Georgia, the draft of which shall be presented by the Ministry of Justice of Georgia in consultation with the Ministry of Defense and the Ministry of Internal Affairs. The list should be drafted according to the following criteria: potential severity and scope effects caused by downtime or destruction of an information system in relation to defense capabilities of the state; potential economic impact on the subject and the state; degree of viability of the information system for the uninterrupted functioning of the defense; number of users of the system; economic state of the subject in question and cost of compliance with obligations deriving from the law.

5. Statute and structure of the Cyber Security Bureau are approved by the Minister of Defense of Georgia.

6. The main function of the Cyber Security Bureau is to exercise activities within the scope of authority vested upon by the law, including this Law.

7. Provisions of Articles 6 and 7, par. 4 of Article 9 and par. 2 of Article 2 do not apply to the Cyber Security Bureau.

Article 10^2. Director of the Cyber Security Bureau

1. Director of the Cyber Security Bureau is appointed to and removed from this post by the Minister of Defense of Georgia.

2. Director of the Cyber Security Bureau is supported by two Deputies, one of whom is the First Deputy who exercises the authority of the Director in his/her absence. Deputy Directors are appointed to and removed from this post by the Director of the Cyber Security Bureau with the approval of the Minister of Defense of Georgia.

3. Director of the Cyber Security Bureau is performing duties within the scope of authority vested upon by this Law and Statue of the Cyber Security Bureau.

4. Director of the Cyber Security Bureau is entitled to appoint to and remove from post the personnel of the Cyber Security Bureau in the manner provided by the law of Georgia.

5. Director of the Cyber Security Bureau is entitled to issue normative acts – orders in cases and within the scope provided by this Law and other legal acts of Georgia. Normative acts regulating defense policies in cyber security are issued by the Minister of Defense of Georgia.

6. Staff regulations and payroll of the Cyber Security Bureau are approved by the Minister of Defense of Georgia in the manner provided by the Georgian law.

Article 10^3. Computer Incident Response Team of the Cyber Security Bureau

1. The Computer Incident Response Team of the Cyber Security Bureau – CERT.MOD.GOV.GE (hereinafter - Computer Incident Response Team of the Cyber Security Bureau) handles cyber attacks against defense sphere critical information system subjects which endanger life and health of persons, threaten state interests and defense capabilities, as well as other performs management of other information security incidents and related activity that aims to resolve priority threats against cyber security.

2. Priority threats and responsibilities of the Computer Incident Response Team of the Cyber Security Bureau are determined by the Article 8, par. 2 and 3 of this Law.

Chapter IV. Temporary and Closing Provisions

Article 11. Temporary provisions

1. The President of Georgia shall adopt a Decree on "Approval of the List of Critical information system Subjects" within 6 months from entry of this Law into force.

2. Within 6 months from entry of this Law into force, the Data Exchange shall adopt the following normative acts:

a) Order on „Computer Emergency Response Team of the Data Exchange Agency“;

b) Order on „Approval of Minimum Standards for Information Security Officer of the Critical Information System Subject";

c) Order on “Configuration of Network Sensor in the Network of the Critical information system Subject”;

d) Order on “Minimum Requirements of Information Security”;

e) Order on “Approval of Rules for Authorization of Persons and Organizations Eligible to Perform Information Security Audit, Authorization Procedures and Costs”;

f) Order on “Rules for Conducting Information Security Audit”;

g) Order on “Approval of Rules on Information Assets Management”.

3. The Government of Georgia shall adopt, by 1 April 2014, a decree on “Approving the List of Critical Information System Subjects”.

4. Before adoption of the Decree provided by the preceding paragraph, the Order 157 of the President of Georgia of 11 March 2013 “On Approving the List of Critical Information System Subjects” shall remain legally applicable.

5. The Ministry of Defense of Georgia, by 1 April 2014, shall undertake appropriate actions provided by Law in order to establish the Cyber Security Bureau.

6. The Minister of Defense of Georgia, by 1 April 2014, shall issue the following normative acts:

a) Order on “Computer Emergency Response Team of the Legal Entity of Public Law – Cyber Security Bureau”;

b) Order on “Minimum Requirements of Information Security”;

c) Order on “Approval of Rules on Information Assets Management”.

Article 12. Closing provision

This Law shall enter into force on 1 July 2012.