LAW OF GEORGIA

ON INFORMATION SECURITY

Chapter I - General Provisions

Article 1 - Purpose of the Law

This Law aims to promote the efficient and effective maintenance of information security, define rights and responsibilities for public and private sectors in the field of information security maintenance, and identify the mechanisms for exercising state control over the implementation of information security policy.

Article 2 - Definition of terms

The terms used in this Law shall have the following meanings:

a) **information security** – an activity that ensures the protection of access to, integrity, authenticity, confidentiality, and non-repudiation of information and information systems;

b) **information security policy** – a set of the standards, principles, and practices laid down in this Law, other normative acts and international treaties of Georgia, that ensures information security and complies with the international standards established within the scope of its maintenance;

c) **cyberspace** – a domain characterized by the use of electronics and electromagnetic spectrum to store, modify, or exchange data via networked systems and an associated physical infrastructure;

d) **cyber-attack** – an action when an electronic device and/or a network or a system connected thereto is used through disrupting, impeding, or destroying the integrity of the systems, property or functions within the critical information system, or through obtaining information illegally;

e) **computer incident** – an actual or potential violation of information security policy by using an information technology that causes an unauthorized access to, disclosure, damage or impediment of information, or theft of information resources;

f) **critical information system** – an information system whose uninterrupted operation is essential to national defence and/or economic security, as well as to normal functioning of the state authority and/or society;

g) **critical information system subject** – a state body or a legal person whose uninterrupted operation of the information system is essential to the defence and/or economic security of the State, as well as to the maintenance of state authority and/or public life;

h) **confidential information** – information, the breach of confidentiality, integrity or availability of which may cause a substantial damage to the functions of the critical information system subject. The purpose of classifying information as confidential is to provide rules for the information asset management, except for the rules defining access to public information set forth by the General Administrative Code of Georgia;

i) **information for internal use** – information designated only for employees and/or contractors of the critical information system subject. The breach of the confidentiality, integrity, or availability of this information may cause a substantial disruption of the operation of the critical information system subject, or impair the security of public authorities, state interest, or business reputation of a private person. The purpose of classifying information as information for internal use is to provide the rules for information asset management, except for the rules defining access to public information set forth by the General Administrative Code of Georgia;

j) **information asset** – all information and knowledge (particularly, technological means for the storage, processing, and transfer of information, personnel and their knowledge of information processing) that is valuable to the critical information system subject;

k) **information system** – any combination of information technology and actions carried out by using such technology that facilitates the management and/or decision-making;

l) **network sensor** – a device specifically designed for monitoring a network segment in order to identify the actions that indicate the attack against or intrusion into the information system;

m) **Data Exchange Agency**– a legal entity under public law within the governance of the Ministry for Justice of Georgia ('Data Exchange Agency');

n) **Cyber Security Bureau** - a legal entity under public law within the Ministry for Defence of Georgia ('Cyber Security Bureau');

Law of Georgia No 1829 of 24 December 2013 – website, 28.12.2013

Article 3 - Scope of the Law

1. This Law shall apply to all legal persons and state authorities that are critical information system subjects. This Law shall also apply to the organisations and agencies that are subordinated or related to the critical information system subject through labour, internship, contractual, or other relationships and that provide access to information assets under such relationships.

2. The list of critical information system subjects and the criticality classification for the respective subjects shall be approved by an ordinance of the Government of Georgia. The Ministry of Justice of Georgia, in agreement with the Ministries of Defence and Internal Affairs of Georgia and the State

Security Service of Georgia shall submit the draft ordinance to the Government of Georgia for approval. The list shall be compiled according to the following criteria: the gravity and scale of potential consequences resulting from the malfunction or the failure of an information system; the gravity of expected economic losses for information system subjects and/or the State; the necessity of services delivered by the information system for the normal functioning of society; the number of information system users; material standing of the subject concerned; and the amount of estimated costs incurred as a result of the liabilities imposed by this Law.

3. This Law shall not apply to mass media, editorial offices of publishing houses, scientific, educational, religious, and public organisations, as well as to political parties regardless of the importance of their activities to the national defence and/or economic security and to the maintenance of state authority and/or public life.

4. Any legal person and public authority that is not a critical information system subject, may voluntarily assume the obligations deriving from this Law.

5. This Law shall not apply to any action permitted in advance by the consent of the critical information system subject that aims to test the information security.

6. The provisions of this Law shall not affect the application of the norms provided for by the legislation of Georgia that governs freedom of information, personal data processing, protection of state, commercial, and private secrets.

Law of Georgia No 1250 of 20 September 2013 – website, 1.10.2013

Law of Georgia No 1829 of 24 December 2013 – website, 28.12.2013
Law of Georgia No 3933 of 8 July 2015 – website, 15.7.2015

Chapter II - Organisation and Provision of Information Security

Article 4 - Rules for information security

1. A critical information system subject shall be obliged to adopt internal rules for information security that serve to enforce the provisions of this Law and to define information security policy of the entity concerned.

2. Information security policy shall meet the minimum requirements for information security (based on the criticality classification of the critical information system subject) that are defined by the Data Exchange Agency in accordance with the standards and requirements laid down by the International Organisation for Standardisation (ISO) and the Information Systems Audit and Control Association (ISACA).

3. The critical information system subject shall submit internal rules for information security adopted pursuant to the first paragraph of this article to the Data Exchange Agency for review. The Data Exchange Agency shall also be notified of any changes made to the internal rules for information security. The Data Exchange Agency shall carry out a general analysis of the documents submitted in that manner and present recommendations for eliminating any deficiencies identified.

4. In addition to the documents set forth under the third paragraph of this article, the Data Exchange Agency shall have no access to the information or information assets of the critical information system subject, unless the critical information system subject voluntarily provides the Data Exchange Agency with the access to the information and information assets.

Law of Georgia No 1829 of 24 December 2013 – website, 28.12.2013

Article 5 - Information Asset Management

1. Under the internal rules provided for by Article 4(1) of this Law, a critical information system subject shall take inventory of information systems to keep record of all information assets. As a result, each information asset will be assigned the respective criticality class - confidential or for internal use. All other information assets that do not require classification shall be considered open information.

2. The inventory of information assets will result in the description of all information assets according to their significance, value, current level of security and protection.

3. While creating an information asset, the asset creator and/or the person responsible for the asset shall determine the respective criticality class.

4. The Data Exchange Agency shall, lay down the rules for the information asset management by a normative act, in particular, the rules for their inventory, classification, availability, issuance (publication), change, and destruction, except for the rules by which the General Administrative Code of Georgia defines the accessibility to public information.

Article 6 - Information security audit and information systems testing

1. By the consent of the critical information system subject, the Data Exchange Agency or a person or an organisation selected by the critical information system subject from among the persons authorised by the Data Exchange Agency shall assess the compatibility of the internal rules for information security (information security policy) with the minimum security standards established by the Data Exchange Agency (information security audit). After the audit, a report shall be drawn up. The requirements laid down in the report shall be fulfilled.

2. The Data Exchange Agency shall lay down the rules for conducting the information security audit laid down in the first paragraph of this article by a normative act.

3. The price for the information security audit conducted by the Data Exchange Agency shall be fixed under a contract concluded with the critical information system subject.

4. The Data Exchange Agency shall lay down, by a normative act, the authorisation rules for the persons and agencies entitled to conduct information security audit, authorisation procedures, and cost.

5. The Data Exchange Agency, with the consent of the critical information system subject or an independent, competent person or agency selected by the critical information system subject with the prior permission of the Data Exchange Agency shall carry out penetration testing and vulnerability assessment of the information system according to the pre-scheduled and documented task.

6. If an audit or testing provided for by this article identifies non-compliance with the information security policy requirements, the critical information system subject shall analyse the cause for such non-compliance and, if necessary, shall determine and carry out relevant corrective measures, and shall submit their schedule to the Data Exchange Agency.

Article 7 - Information security manager

1. The critical information system subject shall be obliged to determine the person(s) or the employee(s) (Information Security Manager) responsible for observing the information security requirements of the critical information system subject.

2. An Information Security Manager shall have the following basic duties:

a) daily monitoring of the compliance with the information security policy requirements;

b) providing assessment of information assets and their availability;

c) drafting internal information security policy documentation;

d) collecting information on information security incidents and monitoring responses to such incidents;

e) reporting on information security issues and other administrative/organizational activities;

f) organizing and conducting general and sectorial trainings on information security;

g) other duties defined by the critical information system subject.

3. An Information Security Manager shall be accountable to the head of the critical information system subject or its duly authorised employee, or a group of persons (collegiate body) entitled to implement information security policy. All major decisions concerning the implementation of information security policy shall be made by the person(s) specified under this paragraph or by a prior consent of the same person(s).

4. An Information Security Manager shall draft an action plan for information security and present an annual progress report to the person(s) specified under the third paragraph of this article, and to the Data Exchange Agency.

Chapter III - Ensuring Cyber Security

Article 8 - Computer Emergency Response Team of the Data Exchange Agency

1. The Computer Emergency Response Team of the Data Exchange Agency – CERT.GOV.GE ('CERT') shall be responsible for the enforcement of the provisions of this Law, in particular, the management of the incidents against information security in the cyberspace of Georgia, as well as other related activities aimed to coordinate information security that serves to eliminate priority cyber security threats.

2. Priority cyber security threats shall include:

a) a cyber-attack that threatens human life and health, state interests or defence capacity of the country;

b) a cyber-attack against the information systems of the critical information system subject;

c) a cyber-attack that threatens the financial resources and/or property rights of a state, an organisation or a private person;

d) any other action that, based on its nature, purpose, source, scale or quantity, or the amount of resources required for its prevention, contains sufficient threat for proper functioning of the critical information system.

3. CERT duties shall include:

a) giving recommendations on maintaining information security of the critical information system;

b) detecting computer incidents in a timely manner;

c) responding to computer incidents and coordinating the responses to such incidents;

d) recording computer incidents, as well as establishing and categorizing their response priorities;

e) analysing computer incidents;

f) providing assistance in the process of remedying the consequences of computer incidents and minimising the inflicted damage;

g) coordinating the computer incident prevention measures and providing assistance in the implementation of such measures;

h) raising awareness of information security issues, including providing information on existing threats and weak points within the critical information systems, unless the availability of such information poses a threat to the information security;

i) warning a wide circle of users about potential threats and providing relevant information to them;

j) providing educational and information support on information security issues;

k) providing representation and coordination on information security issues at international level;

l) performing other duties related to information security objectives that are defined by law or other normative act.

4. CERT may request access to the information asset, information system and/or to any object that is a part of the information infrastructure of the critical information system subject, if such access is necessary for proper response to any current or past computer incident. The Information Security Manager shall notify CERT about the possibility or impossibility of such access after reviewing the request within a reasonable period of time.

5. The Data Exchange Agency shall define CERT's competence, working procedures, computer incident response mechanisms, and other rules of activity by a normative act.

Article 9 - Cyber security specialist

1. The critical information system subject shall be obliged to determine the person(s) or the employee(s) responsible for the practical provision of security for the computer systems of the critical information system subject (Cyber Security Specialist).

2. A Cyber Security Specialist shall have the following basic duties:

a) daily monitoring and assessing computer systems;

b) identifying and responding to computer incidents;

c) providing analysis and reporting of computer incidents and security measures;

d) coordinating with CERT;

e) performing other duties defined by the critical information system subject.

3. A Cyber Security Specialist shall be accountable to the head of information technology service of the critical information system subject, or to the employee duly authorised by the latter.

4. A Cyber Security Specialist shall be available at any time, including the time after working hours. He/she shall ensure regular coordination with the Data Exchange Agency during the ongoing or potential cyber-attacks against the critical information system subject, as well as in the process of eliminating the effects of such cyber-attacks.

5. If an ongoing or a potential cyber-attack poses an exceptional threat to the defence capacity or economic security of the country, as well as to the proper functioning of state authority and/or society, the Data Exchange Agency shall be authorised to temporarily coordinate cyber security specialists to prevent, repel the attack, and/or eliminate its consequences.

Article 10 - Computer incident identification

1. The critical information system subject shall identify computer incidents that imply the study and description of each incident and the response thereto.

2. In agreement with the critical information system subject, the Data Exchange Agency and a Cyber Security Specialist shall configure and manage the network sensor (system of sensors) required for the identification and examination of computer incidents in the network of the critical information system subject. The Data Exchange Agency shall determine the configuration rules for network sensors by a normative act.

3. CERT shall be immediately notified of the identified computer incident and, if necessary, urgent measures shall be taken in order to preserve and protect incident-related information.

4. While performing the duties provided for by this Law, CERT shall study and describe computer incidents and adequately respond to them.

Chapter III[1] - Cyber Security Bureau

Law of Georgia No 1829 of 24 December 2013 – website, 28.12.2013

Article 10^1 - Status and functions of the Cyber Security Bureau

1. The information security policy for critical information system subjects in the field of defence shall meet the minimum requirements for information security in the field of defence (taking into account the criticality classification of critical information system subject in the field of defence). The Cyber Security Bureau shall define those requirements in accordance with the standards and requirements established by the International Organisation for Standardisation (ISO) and Information Systems Audit and Control Association (ISACA).

2. The Cyber Security Bureau shall be established in accordance with this Law and the Law of Georgia on Legal Entity under Public Law.

3. The scope of activities of the Cyber Security Bureau shall not fall beyond the Data Exchange Agency, whose powers, functions and scope of activity shall be defined by this Law and the Law of Georgia on Data Exchange Agency - Legal Entity under Public Law.

4. The list of critical information system subjects in the field of defence shall be approved and the classification of the relevant subject criticality shall be determined by an appropriate act of the Government of Georgia. The Ministry for Justice of Georgia shall submit the draft act to the Government of Georgia in agreement with the Ministries of Defence and Internal Affairs of Georgia and the State Security Service of Georgia. When making the list, the following criteria shall be taken into account: the severity and scope of the expected results of the information system malfunction or failure in terms of state defence; the severity of economic damage for the subjects and/or the State; the necessity for information system services for smooth functioning of the state defence; the number of information system users; material status of a subject and the amount of expected expenses incurred as a result of imposing relevant obligations on the subject.

5. The Minister for Defence of Georgia shall approve the statute and structure of the Cyber Security Bureau.

6. The main function of the Cyber Security Bureau is to carry out the activities provided for by the legislation of Georgia, including this Law, within the powers granted to it.

7. Articles 6, 7, 9(4), and 10(2) shall not apply to the activity of the Cyber Security Bureau.

Law of Georgia No 1829 of 24 December 2013 – website, 28.12.2013

Law of Georgia No 3933 of 8 July 2015 – website, 15.7.2015

Article 10^2 - Director of the Cyber Security Bureau

1. The Minister for Defence of Georgia shall appoint and dismiss the Director of the Cyber Security Bureau.

2. The Director of the Cyber Security Bureau shall have two Deputies, including one First Deputy performing the duties of the Director in his/her absence. The Director of the Cyber Security Bureau shall appoint and dismiss the Deputy Directors in agreement with the Minister for Defence of Georgia.

3. The Director of the Cyber Security Bureau shall act within the powers granted by this Law and the Statute of the Cyber Security Bureau.

4. The Director of the Cyber Security Bureau may appoint and dismiss the employees of the Cyber Security Bureau in the manner provided for by the legislation of Georgia.

5. The Director of the Cyber Security Bureau shall issue a normative act, an order, in the cases and within the scope defined by this Law and other legislative acts of Georgia. The Minister for Defence of Georgia shall issue normative acts governing the defence policy in the field of cyber security.

6. The Minister for Defence of Georgia shall approve the staff list and salaries for the Cyber Security Bureau in the manner provided for by the legislation of Georgia.

Law of Georgia No 1829 of 24 December 2013 – website, 28.12.2013

Article 10^3 – CERT of the Cyber Security Bureau

1. CERT– CERT.MOD.GOV.GE (the Computer Emergency Response Team) shall manage cyber-attacks against a critical information system subject in the field of defence that endangers the human life and health, the state interests and defence, also shall manage other incidents occurred against the information security and the related activities that serve to eliminate priority threats to cyber security.

2. Priority threats for CERT of the Cyber Security Bureau and the duties of CERT shall be defined in Article 8(2) and (3) of this Law.

Law of Georgia No 1829 of 24 December 2013 – website, 28.12.2013

Chapter IV - Transitional and Final Provisions

Article 11 - Transitional provisions

1. The President of Georgia shall issue an Edict on Approval of the List of Critical Information System Subjects within six months after the enactment of this Law.

2. Within six months after the enactment of this Law, the Data Exchange Agency shall issue the following normative acts:

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

b) Order on Approval of the Minimum Standards for Information Security Manager of the Critical Information System Subject

c) Order on the Rules for Network Sensor Configuration

d) Order on the Minimum Requirements for Information Security

e) Order on the Procedure for Going through Authorisation for Persons and Organisations Entitled to Conduct Information Security Audit, the Authorisation Procedures, and the Authorisation Fees

f) Order on the Information Security Audit Procedure

g) Order on the Rules for Information Asset Management.

3. The Government of Georgia shall adopt Resolution on the Approval of the List of Critical Information System Subjects before 1 April 2014.

4. Until the resolution referred to in the third paragraph of this article is adopted, the Edict No 157 of 11 March 2013 of the President of Georgia on the Approval of the List of Critical Information System Subjects shall remain in force.

5. The Ministry for Defence of Georgia shall take relevant measures under the legislation of Georgia to establish the Cyber Security Bureau before 1 April 2014.

6. The Ministry for Defence of Georgia shall issue the following normative acts before 1 April 2014:

a) Order on Computer Emergency Response Team - Legal Entity under Public Law of Cyber Security Bureau

b) Order on the Minimal Requirements for Information Security

c) Order on the Rules for Information Asset Management.

Law of Georgia No 1250 of 20 September 2013 – website, 1.10.2013

Law of Georgia No 1829 of 24 December 2013 – website, 28.12.2013

Article 12 - Final provision

This Law shall enter into force as from 1 July 2012.

President of Georgia **M. Saakashvili**

Tbilisi

5 June 2012

№6391- IS