Text consolidated by Valsts valodas centrs (State Language Centre) with amending laws of:
1 November 2012 [shall come into force from 1 January 2013];
6 November 2013 [shall come into force from 1 January 2014];
5 February 2015 [shall come into force from 4 March 2015].
If a whole or part of a section has been amended, the date of the amending law appears in square brackets at the end of the section. If a whole section, paragraph or clause has been deleted, the date of the deletion appears in square brackets beside the deleted section, paragraph or clause.

The Saeima[1] has adopted and
the President has proclaimed the following Law:

Law On the Security of Information Technologies

Section 1. Purpose of This Law

(1) The purpose of this Law is to improve the security of information technologies, laying down the most important requirements in order to guarantee the receipt of such essential services, in the supply of which such technologies are used.
(2) The security of information technologies shall be guarded in such a way that it is possible to make early forecasts and to prevent, as well as to overcome danger to such security and eliminate the consequences thereof.
(3) Within the meaning of this Law information technologies are technologies, which perform electronic processing of information, including creation, deletion, storage, display or forwarding, for execution of the tasks provided for such technologies.

Section 2. Application of this Law

(1) This Law shall apply to State and local government authorities, as well as merchants and other legal persons governed by private law (hereinafter – legal persons governed by private law).
(2) This Law shall not apply to the content of the information transmitted in electronic communications networks (for example, to the content of services of an information society and to audiovisual productions).

Section 3. Critical Infrastructure of Information Technologies

(1) The critical infrastructure of information technologies is an infrastructure, which is approved by the Cabinet in accordance with the National Security Law.
(2) The critical infrastructure of information technologies shall be defended in order to provide the performance of the basic functions essential to the State and society. Moreover, the integrity, availability and confidentiality of the critical infrastructure of information technologies shall be ensured.
(3) The procedures for the planning and implementation of security measures for the critical infrastructure of information technologies shall be stipulated by the Cabinet.

Section 4. Information Technologies Security Incidents Response Institution

(1) The Information Technologies Security Incidents Response Institution (hereinafter – Security Incidents Response Institution) shall promote the security of information

[1] The Parliament of the Republic of Latvia

technologies in the Republic of Latvia. The activities of the Security Incidents Response Institution shall be ensured by the leading State administrative institution in the national defence sector. The operational tasks and rights thereof shall be delegated to the Agency of the University of Latvia "Institute of Mathematics and Computer Science of the University of Latvia", which executes such tasks and exercises its rights under the subordination of the relevant State administrative institution in accordance with the funds allocated from the State budget and the conditions of the delegation contract. The leading State administrative institution in the national defence sector shall implement the subordination in accordance with laws and regulations and the provisions of the delegation contract, including controlling an efficient execution of the delegated tasks, giving instructions regarding execution thereof and requesting the necessary information.

(2) Persons shall be employed in the Security Incidents Response Institution within the framework of the service or legal employment relationship, if they are entitled to receive a special permit for access to an official secret and comply with other requirements stipulated in legal acts. Persons employed in the Security Incidents Response Institution, upon performing delegated tasks, shall observe the principles of law and shall be responsible for the legality of their act or omission.

(3) The Security Incidents Response Institution is not entitled to request any payment for activities related to the execution of the functions laid down in this Law.

(4) State and local government authorities and legal persons governed by private law have a duty to co-operate with the Security Incidents Response Institution, providing it with the necessary information and implementing its lawful requests.

(5) In case of danger to the State the Cabinet may take a decision to transfer the tasks, rights and resources of the Security Incidents Response Institution to the National Armed Forces.

(6) Contestation or appeal of administrative acts issued for exercising of the rights laid down in this Law for the prevention of direct danger to the State security or the security of information technologies shall not suspend the operation of such acts. It shall not apply to administrative acts regarding the imposition of administrative punishments.

(7) When taking administrative decisions, the Security Incidents Response Institution shall conform to the requirements of the State Administrative Structure Law.

[1 November 2012]

Section 5. Tasks and Rights of the Security Incidents Response Institution

(1) The Security Incidents Response Institution shall:

1) maintain a unified representation of activities in progress in the electronic information space;

2) provide support for the prevention of an information technologies security incident or co-ordinate the prevention thereof;

3) maintain, in a publicly accessible way, recommendations regarding the prevention of the current risks of information technologies, drawn up in accordance with the current threats;

4) conduct research work, organise educational measures, training and instruction in the field of the security of information technologies;

5) provide support to State authorities in the protection of State security, as well as detection (investigation) of criminal offences and other violations of the law in the field of information technologies, conforming to the restrictions laid down in the laws and regulations regarding data processing;

6) supervise how State and local government authorities and electronic communications merchants fulfil the duties laid down in this Law;

7) co-operate with internationally recognised information technologies security incidents response institutions (teams);

8) fulfil other duties laid down in laws and regulations.

(2) The Security Incidents Response Institution is entitled to:

1) request and receive from State and local government authorities and legal persons governed by private law technical information regarding an information technologies security incident that has taken place or an ongoing information technologies security incident (information regarding the scope of the incident, malicious software files that have caused the incident, description of vulnerabilities, technical measures performed for the prevention of the incident, information regarding activities performed by persons doing harm or other technical information, including IP addresses);

2) obtain from State and local government authorities and legal persons governed by private law, upon mutual agreement, online data flow;

3) carry out testing of the critical infrastructure of information technologies;

4) take decisions (also issue administrative acts) in order to ensure the fulfilment of the duties laid down in this Law for State and local government authorities, as well as legal persons governed by private law.

[5 February 2015]

Section 6. Actions in the Event of an Information Technologies Security Incident

(1) An information technologies security incident (hereinafter – security incident) is a harmful event or offence, as a result of which the integrity, availability or confidentiality of information technologies is endangered.

(2) In case of a security incident a State or local government authority, the owner or lawful possessor of the critical infrastructure of information technologies shall perform all activities necessary for the prevention thereof (particularly fulfil the recommendations of the Security Incidents Response Institution regarding the preferable initial action in case of a security incident), as well as inform the Security Incidents Response Institution thereof without delay. The Security Incidents Response Institution shall come to an agreement with the applicant of the security incident regarding the provision of support in prevention of the security incident.

(3) In case of a security incident legal persons governed by private law, to whom the duties laid down in Paragraph two of this Section are not applicable, shall perform all activities necessary for the prevention thereof and may, upon their own initiative, inform the Security Incidents Response Institution regarding what happened. The Security Incidents Response Institution shall come to an agreement with the applicant of the security incident regarding the provision of support in prevention of the security incident.

(4) The Security Incidents Response Institution, having detected a security incident, which jeopardises national security, shall inform the Minister for Transport, the Minister for Defence, the minister responsible for the sector and the competent State security institution thereof, as well as shall submit proposals for the necessary actions, but, if such breach of security or integrity has been detected, which has had a significant impact on the operations of electronic communications networks or the provision of services, may notify the State administrative institutions of the European Union Member States and the European Network and Information Security Agency regarding what happened. The Security Incidents Response Institution may inform the public or require the relevant electronic communications merchants to do so, where it determines that disclosure of the breach is in the public interest.

[1 November 2012; 5 February 2015]

Section 6.[1] Action in Case of Detecting an Information Technologies Security Vulnerability

(1) An information technologies security vulnerability (hereinafter – security vulnerability) is an essential systemic weakness caused intentionally or unintentionally during establishment,

maintenance or modification of an information system or electronic communications network, as a result of which the integrity, accessibility or confidentiality of information technologies may be endangered.
(2) Having detected a security vulnerability, the State or local government authority, the owner or lawful possessor of the critical infrastructure of information technologies shall, within 90 days, perform all the actions necessary for elimination thereof, as well as inform the Security Incidents Response Institution thereof without delay.
(3) Having detected a security vulnerability, the Security Incidents Response Institution shall inform the owner or lawful possessor of the information system or electronic communications network regarding the fact without delay. The State or local government authority, the owner or lawful possessor of the critical infrastructure of information technologies shall, within the time period stipulated by the Security Incidents Response Institution, but not later than within 90 days from the moment of informing, perform all the actions necessary for elimination of the security vulnerability.
[5 February 2015]

Section 7. Processing of Personal Data

(1) The Security Incidents Response Institution has the right to receive and process personal data in order to substantiate or exclude suspicions regarding a security incident or to prevent it, if it is not possible to anonymise personal data and at least one of the following conditions exists:
1) malicious software may contain personal data;
2) personal data is being transmitted, using malicious software;
3) personal data may provide essential information regarding malicious software.
(2) If a security incident is detected, processing of personal data shall be allowed in order to provide protection from malicious software or the consequences caused thereby, as well as to detect other malicious software and ensure protection against it.
(3) The Security Incidents Response Institution shall be allowed to transfer processed personal data to the institutions (units) referred to in Section 5, Paragraph one, Clauses 5 and 7 of this Law in order to recognise and prevent activities of such malicious software, which may cause or causes threats to the national or public security.
(4) The Security Incidents Response Institution shall be allowed to perform processing of personal data, which is not related to the prevention of such incident, due to which such data was obtained, only if it prepares and sends the State Data Inspectorate a description of the planned processing and protection of personal data. The Security Incidents Response Institution shall, by 20 January of the following year, prepare and submit to the State Data Inspectorate a report on the processing of personal data performed during the previous year.

Section 8. Security of Information Technologies of State and Local Government Authorities

(1) The management of the security of information technologies of State and local government authorities shall be ensured by the head of each relevant authority.
(2) The head of a State or local government authority shall appoint the responsible person who implements the management of the security of information technologies in the relevant authority (hereinafter – responsible person). The Security Incidents Response Institution shall, not later than within five working days, be informed regarding the appointing of the responsible person.
(3) In addition to the duties laid down in other legal acts the responsible person has the following duties:

1) to organise the management of the security of information technologies of the authority;

2) not less than once a year to perform examination of the security of information technologies and in accordance with the results thereof organise elimination of the deficiencies detected;

3) at least once a year to attend training organised by the Security Incidents Response Institution in matters of the security of information technologies;

4) not less than once a year to instruct the staff of the authority on matters of the security of information technologies.

(4) Each State or local government authority, taking into account that prescribed by this Law and other laws and regulations, shall ensure that regulated provisions for the security of information technologies exist in the authority, which include at least descriptions and charts of information technologies, risk analysis of information technologies, plan for the management of information technologies risk and security incidents, lay down the duties of the persons involved in the maintenance of information technologies, as well as ensure that the fulfilment of this Regulation is constantly monitored and controlled.

(5) The Cabinet shall determine the minimum requirements for information and communication technologies, and the procedures by which State and local government authorities shall ensure the conformity of information and communications technologies systems with the minimum safety requirements.

[5 February 2015]

Section 9. Security of Public Electronic Communications Networks

(1) Electronic communications merchants have the following duties:

1) if the relevant merchant provides a public electronic communications network – to ensure the integrity of the network, thus achieving continuity of supply of services, as well as to draw up an action plan for ensuring continuous operation of the electronic communications network, indicating therein the technical and organisational measures to appropriately manage the risks posed to security of the network and the provision of services;

2) to inform the Security Incidents Response Institution regarding breaches of security or integrity, which have had a significant impact on the operation of the electronic communications network or the provision of services. An incident, as a result of which the electronic communications network does not operate for at least 24 consecutive hours, shall be deemed an essential breach of security or integrity;

3) upon request of the Security Incidents Response Institution to provide it with the information necessary for evaluation of security and integrity of services and the network, including a documented security policy;

4) upon request of the Security Incidents Response Institution, if essential breaches of security and integrity have been detected, to organise a security audit to be carried out by a qualified body governed by public law, which has been co-ordinated with the Security Incident Response Institution and is independent of the parties involved. The Security Incidents Response Institution shall be informed regarding the results of the audit. The breaches determined in the audit shall be eliminated and costs of the audit shall be paid by the electronic communications merchant;

5) upon request of the Security Incidents Response Institution to disconnect the end user from the electronic communications network for a short period of time, but not longer than for 24 hours, if the end user significantly endangers the rights of other users or the information system, or the security of the electronic communications network. When requesting the performance of such activity, the Security Incidents Response Institution shall indicate the reason for the request.

(2) The Cabinet shall determine the information to be included in the action plan for the provision of continuous operation of the electronic communications network, the procedures for control of the implementation of such plan and the procedures, by which end users shall be temporarily disconnected from the electronic communications network.

Section 10. National Council for the Security of Information Technologies

In order to co-ordinate the drawing up of the policy related to the security of information technologies, as well as the planning and carrying out of the relevant tasks and measures, the Prime Minister shall establish a National Council for the Security of Information Technologies, the operation of which shall be ensured by the leading State administrative institution in the national defence sector.
[6 November 2013]

Transitional Provisions

1. Section 9 of this Law shall come into force on 1 May 2011.

2. The Cabinet shall issue the regulations provided for in Section 3, Paragraph three of this Law by 1 February 2011.

3. The Cabinet shall issue the regulations provided for in Section 9, Paragraph two of this Law by 1 May 2011.

4. The Prime Minister shall establish the National Council for the Security of Information Technologies specified in Section 10 of this Law by 1 February 2011.

5. The Cabinet shall issue the regulations provided for in Section 8, Paragraph five of this Law by 15 March 2015.
[5 February 2015]

Informative Reference to the European Union Directive

This Law contains legal norms arising from Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2009/20/EC on the authorisation of electronic communications networks and services.

This Law shall come into force on 1 February 2011.

This Law was adopted by the Saeima on 28 October 2010.

President V. Zatlers

Adopted 10 November 2010