

Procedure for Protection of State Secrets and Classified Information of Foreign States

Government of the Republic Regulation No. 262 of 20 December 2007

RTI, 28.12.07, 73, 449

Entered into force 01.01.2008

This Regulation is established based on subsection 11 (1), subsection 13 (5), subsection 14 (4), subsections 15 (4) and (5), subsections 20 (4) and (6), subsection 27 (13), subsection 31 (5), subsection 36 (3), subsection 39 (1), subsection 41 (6), subsection 42 (4), subsection 46 (4) and subsection 51 (6) of the State Secrets and Protection of State Secrets and Classified Information of Foreign States Act.

Chapter 1

General Provisions

§ 1. Scope of application of Regulation

This Regulation establishes the procedure for the protection of state secrets and classified information of foreign states, and the subcategories of information classified as a state secret, and the levels and terms of classification of subcategories of information.

§ 2. Definitions

In this Regulation, the following definitions are used:

- 1) classified information - state secrets, or classified information of foreign states;
- 2) processing unit - agencies, constitutional institutions and legal persons which process classified information, or natural persons who process classified information based on a processing permit;
- 3) administrative area - an area with clear external borders used by a processing unit, whereas all persons and vehicles which enter such area must be identified;
- 4) public area - an area which is not a security area or an administrative area;
- 5) correction of classification data - declassification of information which has been processed as state secret without a legal basis; correction of the level, legal basis or term of classification of a state secret that has been classified on an incorrect legal basis or for an incorrect term;
- 6) open storage area - a security area where the use of safes, lockable cabinets or drawers is not required;
- 7) courier - a person who forwards classified media.

§ 3. Authorisation of secretary generals of ministries

A minister may authorise the secretary general of the ministry to perform all acts and take all decisions which the minister, as the head of the authority, is authorised to perform and take.

Chapter 2

Subcategories of State Secrets

§ 4. Subcategories of state secrets related to foreign relations

(1) With respect to information related to international relations created by bodies conducting foreign relations and information created by bodies conducting foreign relations, the disclosure of which would significantly damage the foreign relations of the Republic of Estonia, the following shall be a state secret:

- 1) information received by an employee or representative of a body conducting foreign relations during an international meeting or information related to such meeting, the disclosure of which may significantly damage national security. Such information shall be classified as secret for fifty years;
- 2) information received by an employee or representative of a body conducting foreign relations during an international meeting or information related to such meeting, the disclosure of which may damage national security or significantly damage foreign relations. Such information shall be classified as restricted until the arrival of the date or event agreed upon by the parties participating in the meeting however, not for longer than for fifty years;
- 3) information created by a body conducting foreign relations related to the preparation and conduct of international negotiations or meetings, the disclosure of which before the holding of the negotiations or meetings may damage national security or significantly damage foreign relations. Such information shall be classified as restricted until the holding of the meeting, or for fifty years if the disclosure of the information after the meeting or in the case of cancelling the meeting would damage national security or significantly damage foreign relations;
- 4) information concerning the preparation or conduct of international visits or ceremonies (hereinafter in this clause events) unless the disclosure of such information damages national security or significantly damages foreign relations. Such information shall be classified as restricted until the holding of the event, or for fifty years if the disclosure of the information

after the event or in the case of cancelling the event would damage national security or significantly damage foreign relations;

5) information received during an international meeting or information concerning such meeting created by a body conducting foreign relations which is subject to protection against disclosure according to international practices, or whose protection has been agreed upon by the participants in the meeting or other event. Such information shall be classified at the level and for the term determined on an agreement between the participants or pursuant to international practices, however not on a level of classification higher than secret and not for longer than for fifty years;

6) information created by a body conducting foreign relations which concerns international relations, a foreign state or international organisation or a representative thereof, if disclosure of the contents of the information, the manner of forwarding or the source of the information would damage national security or significantly damage foreign relations. Such information shall be classified as restricted for 50 years.

(2) With respect to information collected and prepared by the Strategic Goods Commission operating at the Ministry of Foreign Affairs concerning the import, export and transit of strategic goods, export of services related to military goods, and the end use of strategic goods, the following shall be a state secret:

1) information about the import, export and transit of strategic goods, the export of services related to military goods and end-use of strategic goods collected by the Strategic Goods Commission, except information the disclosure of which would not damage or the security of the Republic of Estonia. Such information shall be classified as secret for 30 years;

2) information about the import, export and transit of strategic goods, the export of services related to military goods and end-use of strategic goods collected by the Strategic Goods Commission, which analyses the dissemination of strategic goods and related danger to security. Such information shall be classified as confidential for 30 years;

3) information concerning refusal by the Strategic Goods Commission to issue an import or export licence, transit permit or document on supervision of end-use of military goods, except for materials, construction works and equipment related to weapons of mass destruction, forwarded to an international control system of strategic goods control - Wassenaar Arrangement Participating States - and the EU Working Group on Conventional Arms Export; as well as information concerning the contents of the meeting of the Strategic Goods Commission which discussed such refusal. Such information shall be classified as restricted for 10 years;

4) information concerning refusal to issue an import or export licence, transit permit or document on supervision of end-use of materials, construction works and equipment related to weapons of mass destruction prepared by the Strategic Goods Commission and forwarded to the international strategic goods control system - the Nuclear Suppliers' Group and the Australia Group; as well as information concerning the contents of the meeting of the Strategic Goods Commission which discussed such refusal. Such information shall be classified as confidential for 20 years.

§ 5. Subcategories of state secrets related to national defence

(1) With respect to information concerning the preparation, management and operations of national defence, the following shall be a state secret:

- 1) inclusion of the personnel and equipment of the Defence Forces in war-time units of the operational structure of the Defence Forces. Such information shall be classified as confidential for 20 years or until the declaration of mobilisation;
- 2) the composition of a type war-time unit of the Defence Forces and information concerning the description of its functions. Such information shall be classified as restricted for 20 years;
- 3) information concerning operative planning of state-wide defence activities of the Defence Forces. Such information shall be classified as secret for 50 years;
- 4) information concerning operative planning of the defence activities of the Defence Forces within a defence district. Such information shall be classified as confidential for 30 years;
- 5) information concerning operative planning of the defence activities of the Defence Forces within a formation centre or war-time unit. Such information shall be classified as restricted for 30 years;
- 6) the action plan of the Defence Forces in the state of emergency. Such information shall be classified as secret for 20 years. Classification shall expire upon use of the public use of the information in the state of emergency;
- 7) the state-wide action plan of the Defence Forces in the case of high readiness, initial full readiness or full readiness. Such information shall be classified as secret for 50 years;
- 8) the action plan of the Defence Forces in the case of high readiness, initial full readiness or full readiness within a defence district. Such information shall be classified as confidential for 30 years;

- 9) the action plan of the Defence Forces in the case of high readiness, initial full readiness or full readiness within a formation centre or war-time unit. Such information shall be classified as restricted for 30 years;
 - 10) information concerning the participation in, direction and conduct of a military operation, necessary for the protection of units. Such information shall be classified as confidential for 10 years;
 - 11) information concerning the war-time structure and control system of the Defence Forces. Such information shall be classified as confidential for 20 years;
 - 12) information concerning the structure of war-time information and communications systems of the Defence Forces, and related protective equipment. Such information shall be classified as confidential for 25 years;
 - 13) information concerning war-time radio frequencies. Such information shall be classified as secret for 50 years;
 - 14) the parameters and operational capacity of the data transmission equipment of the marine monitoring systems of the Defence Forces. Such information shall be classified as confidential for 10 years;
 - 15) the measurement results of the magnetic and acoustic fields of military vessels of the Defence Forces. Such information shall be classified as secret for 10 years;
 - 16) the plan for the military protection of ports. Such information shall be classified as confidential for 20 years;
 - 17) the rules for the use of armed force by the Defence Forces. Such information shall be classified as confidential for 10 years.
- (2) With respect to information concerning the preparation and conduct of mobilisation, the relevant set of data entered in the state central register of mobilisation shall be a state secret. Such information shall be classified as secret for 30 years.
 - (3) With respect to information concerning the mobilisation stockpile, the information concerning the general quantities of the mobilisation stockpile shall be a state secret. Such information shall be classified as secret for 10 years.
 - (4) Regarding the information concerning the military weapons and munitions of war of the Defence Forces and the National Defence League, the following shall be a state secret:
 - 1) information concerning the consolidated data and division of the military weapons and munitions of war of the Defence Forces and the National Defence League, except for the information which is subject to disclosure based on an international agreement; Such information shall be classified as secret for 20 years;

- 2) information concerning the inventory of the warehouses housing the military weapons and munitions of war of the Defence Forces and the National Defence League; Such information shall be classified as secret for 20 years;
- 3) tactical data of the weapons systems of the navy, except for the tactical data of coastal defence weapons systems. Such information shall be classified as confidential for 10 years.
- (5) With respect to information collected by radars and surveillance systems, the following shall be a state secret:
 - 1) radar data and the technical parameters and operational capacity of the surveillance systems of the border guard. Such information shall be classified as confidential for 10 years;
 - 2) capacity parameters of surveillance radars of the air forces, the disclosure of which may damage air surveillance. Such information shall be classified as confidential for 10 years;
 - 3) information concerning the electronic warfare capability of radars, and the countermeasures to be taken in the case of electronic warfare. Such information shall be classified as confidential for 10 years;
 - 4) the data processing algorithms, filtered areas and target criteria of radars. Such information shall be classified as confidential for 10 years;
 - 5) the operational status and times for scheduled maintenance of radars and passive surveillance systems. Such information shall be classified as confidential for 10 years;
 - 6) consolidated data on the location of stationary radars, the disclosure of which may damage air surveillance capacity, and the exact geographic location of mobile radars to the accuracy of degree and minute. Such information shall be classified as confidential for 10 years;
 - 7) results of the maintenance and analysis of radars. Such information shall be classified as confidential for 10 years;
 - 8) information concerning crypted secondary radar signals enabling establishment of objects. Such information shall be classified as confidential for 10 years;
 - 9) integrated radar data collected and processed by air surveillance systems. Such information shall be classified as confidential for 5 years;
 - 10) data collected by and processed on the basis of the passive air surveillance system of the air force. Such information shall be classified as secret for 10 years;
 - 11) information concerning the location, operational function and code name of the air defence system. Such information shall be classified as confidential for 10 years;
 - 12) information concerning the responsibility and surveillance areas of air surveillance. Such information shall be classified as confidential for 10 years;

- 13) information concerning the operational functions of the air defence system. Such information shall be classified as confidential for 10 years;
 - 14) the operational status of the air surveillance system. Such information shall be classified as confidential for 10 years;
 - 15) equipment used in the passive surveillance system and technical parameters thereof. Such information shall be classified as restricted for 10 years;
 - 16) Data collected and analysed by marine surveillance equipment. Such information shall be classified as secret for 10 years;
 - 17) information concerning the capacity of the marine surveillance system to identify and analyse recognised maritime pictures. Such information shall be classified as confidential for 10 years;
 - 18) information concerning the settings of marine surveillance systems installed on ships under specific operating conditions. Such information shall be classified as confidential for 10 years.
- (6) With respect to information concerning inventions and research related to national defence and the outcome thereof, information concerning inventions and research related to national defence, except for information whose disclosure does not damage the security of the Republic of Estonia is deemed to be a state secret. Such information shall be classified as secret or at a lower level of classification for up to 15 years.
- (7) With respect to information collected and synthesised by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence, the following shall be a state secret:
- 1) information collected by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence by means of signals intelligence, or information synthesised on the basis thereof which allows the method of collection to be established. Such information shall be classified as top secret for 50 years;
 - 2) information covertly collected by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence, or information synthesised on the basis thereof. Such information shall be classified as secret for 30 years;
 - 3) information specified in subsection (2) of this section if the disclosure thereof would endanger the life or health of persons. Such information shall be classified as top secret for 50 years;
 - 4) information analysed and synthesised by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence based on source data

up the restricted level of classification which concerns national defence and military sources of danger. Such information shall be classified as confidential for 15 years;

5) information analysed and synthesised by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence based on source data up the restricted level of classification which concerns foreign states, international organisations, foreign military factors and operation. Such information shall be classified as restricted for 15 years;

6) information collected by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence in the process of security checks, or information synthesised on the basis thereof. Such information shall be classified as restricted for 30 years.

(8) With respect to information related to the composition, tasks and distribution of the budget of a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence, the following shall be a state secret:

1) the structure and composition a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence. Such information shall be classified as secret for 25 years;

2) the duties of a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence and of the employees thereof, except for information whose disclosure does not damage the security of the Republic of Estonia. Such information shall be classified as secret for 25 years;

3) consolidated data concerning the employees of a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence, and the employees exclusively engaged in the covert collection of information. Such information shall be classified as secret for 25 years.

(9) The data concerning the persons recruited for secret co-operation by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence and undercover agents is a state secret. Such information shall be classified as top secret for 75 years. Classification shall expire twenty years after the death of such person but not earlier than fifty years after classification of the information.

(10) With respect to information concerning the covert collection of information by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence, the following shall be a state secret:

1) the methods and means used for the covert collection of data by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence. Such information shall be classified as secret for 50 years;

2) information concerning the technical means of signals intelligence. Such information shall be classified as secret for 50 years;

3) information concerning signals intelligence objects. Such information shall be classified as top secret for 50 years.

(11) With respect to information concerning the international cooperation of the Defence Forces in the area of intelligence and counter intelligence, the information concerning the international joint intelligence and counter intelligence operations, cooperation projects and partners of the Defence Forces shall be deemed a state secret. Such information shall be classified as secret for 50 years.

(12) Regarding the information concerning military geography of the Defence Forces and the National Defence League, the following shall be a state secret:

1) the Feature Data Dictionary of the Defence Forces in the scale of 1: 50 000, three-dimensional landscape models, processed remote surveillance data. Such information shall be classified as restricted for 10 years;

2) landscape analyses of the strategic and tactical level concerning the territory of Estonia prepared by the Defence Forces, geo-coordinated plans of national defence objects and three-dimensional geographical models of national defence objects prepared by the Defence Forces. Such information shall be classified as confidential for 30 years;

3) landscape analyses of the strategic and tactical level concerning the territory of a foreign state, geo-coordinated plans of national defence objects, processed remote surveillance data and three-dimensional landscape models prepared by the Defence Forces. Such information shall be classified as secret for 30 years.

§ 6. Subcategories of state secret in area of maintenance of law and order

(1) With respect to information collected by surveillance agencies during surveillance, and information concerning the methods, tactics and means used for the collection of such information, the following shall be a state secret:

1) information collected for the conduct of witness protection in the course surveillance. Such information shall be classified as secret for 25 years;

2) information collected by surveillance agencies by way of surveillance. Such information shall be classified as restricted for 25 years. Classification of such information

shall expire to the extent to which it is entered in the criminal file or is communicated to the person who was under surveillance, or the person whose private or family life was violated by surveillance;

- 3) information received from persons recruited for secret cooperation in surveillance by a surveillance agency. Such information shall be classified as restricted for 50 years;
- 4) information collected during surveillance and prepared by the Central Criminal Police which is reflected in the hazard assessments and reviews dealing with organised crime and other serious crime. Such information shall be classified as restricted for 50 years;
- 5) information reflecting the methods, tactics and means used in surveillance, except for information which can be derived from the information collected by surveillance which has been made public lawfully. Such information shall be classified as restricted for 25 years;
- 6) information concerning the remuneration paid to a person who has been recruited for secret co-operation by a surveillance agency, compensations and taxes paid on such sums, and the documents reflecting them. Such information shall be classified as restricted for 25 years;
- 7) information concerning a simulated person or body which may disclose the connection thereof to the surveillance agency. Such information shall be classified as restricted for 25 years.

(2) With respect to information concerning persons who have been recruited for secret co-operation by a surveillance agency and undercover agents, the information concerning the identity of the persons who have been recruited for secret co-operation by a surveillance agency and undercover agents shall be a state secret. Such information shall be classified as restricted for 75 years. Classification shall expire if twenty years have passed since the death of such person but not less than fifty years since classification of the information.

(3) Information concerning police agents of surveillance agencies is a state secret. Such information shall be classified as restricted for 75 years. The classification of such information shall expire to the extent that it is entered in a criminal file. Classification of information not entered in a criminal file shall expire if twenty years have passed since the death of a person specified in this clause but not less than fifty years since the classification of the information;

(4) Regarding the information concerning the structure, staff and tasks of a structural unit of the Central Criminal Police dealing with witness protection, the information concerning the structure and staff of a structural unit of the Central Criminal Police dealing with witness protection, the persons occupying the posts in that unit, and their duties shall be a state secret

to the extent determined by a directive of the head of the Central Criminal Police. Such information shall be classified as secret for 50 years.

(5) Regarding the property at the disposal of a structural unit of the Central Criminal Police dealing with witness protection and the distribution of the budget thereof, the following shall be a state secret:

1) information concerning the means of transport used by a structural unit of the Central Criminal Police dealing with witness protection if disclosure of such information would endanger the application of witness protection or the safety of the structural unit dealing with witness protection or a person placed under protection. Such information shall be classified as confidential for 10 years;

2) information concerning the property used by a structural unit of the Central Criminal Police dealing with witness protection if disclosure of such information would endanger the application of witness protection or the safety of the structural unit dealing with witness protection or a person placed under protection. Such information shall be classified as secret for 25 years;

3) The classification of budget expenditure and reports on the implementation of the budget of a structural unit of the Central Criminal Police dealing with witness protection. Such information shall be classified as secret for 25 years.

(6) Regarding the information concerning the methods and tactics of application of protective measures related to witness protection, the information concerning the methods and tactics of application of protective measures related to witness protection shall be a state secret. Such information shall be classified as secret for 50 years.

(7) Regarding the information concerning the application of the protective measures related to witness protection to a specific person, the following shall be a state secret:

1) the information concerning the application of the protective measures related to witness protection to a specific person, except for information which reflects only the fact of placing such person under witness protection. Such information shall be classified as top secret for 75 years. Classification shall expire if twenty years have passed since the death of a person placed under witness protection but not less than fifty years since classification of the information;

2) The classification of budget expenditure and reports on the implementation of the budget of a structural unit of the Central Criminal Police dealing with witness protection, if they reflect the protective measures applied with respect to a specific person. Such information shall be classified as top secret for 75 years. Classification shall expire if twenty

years have passed since the death of the person placed under witness protection but not less than fifty years since classification of the document.

(8) Regarding the information concerning operation during a state of emergency or state of war described in the national crisis management plan, the information concerning operation during a state of emergency and war-time described in the national crisis management plan, except for information the disclosure of which does not damage the security of the Republic of Estonia, shall be a state secret. Such information shall be classified as top secret for 50 years. Classification shall expire upon the public use of such information during a state of emergency or state of war.

(9) With respect to information concerning guarded objects subject to increased danger within the meaning of the Security Act, and the information concerning the specific requirements for ensuring the security thereof, the list of objects subject to increased risk of physical attack, the risk analysis and the defence plan shall be a state secret. Such information shall be classified as restricted for 20 years.

(10) Regarding the information concerning operation during emergency situations described in the national action plan crisis management plan of the Ministry of Defence and Ministry of the Interior, the information concerning operation during emergency situations described in the crisis management plan of the Ministry of Defence and Ministry of the Interior, except for information the disclosure of which does not damage the security of the Republic of Estonia, shall be a state secret. Such information shall be classified as confidential for 20 years. Classification shall expire upon the public use of the information in an emergency;.

§ 7. Subcategories of state secret regarding security authorities

(1) With respect to information related to the international cooperation of security authorities, the following shall be a state secret:

- 1) information concerning foreign relations prepared by a security authority unless it contains information specified in clauses 2)-4) of this subsection. Such information shall be classified as restricted for 30 years;
- 2) information concerning security cooperation between the security authority and foreign or international organisations unless it contains information specified in clauses 3) and 4) of this subsection. Such information shall be classified as confidential for fifty years unless agreed otherwise. Such information shall not be classified if it has been made public lawfully;

3) covertly collected information to be transmitted in the course of international cooperation of the security authority, and information concerning the exchange of such information. Such information shall be classified as secret for fifty years unless agreed otherwise;

4) information collected covertly by a security authority together with a foreign police or security authority, and information reflecting the collection of information or information exchanged in the course thereof. Such information shall be classified as secret for fifty years unless otherwise agreed.

(2) Regarding the information concerning the property used by a security authority and distribution of the budget of a security authority, the following shall be a state secret:

1) information concerning the property used by a security authority if disclosure of such information would endanger the performance of the functions of the security authority, or the security of the security authority. Such information shall be classified as confidential until the termination of the use of the property or the end of the possession of the building or construction works but not for longer than for twenty five years;

2) information concerning the technical means used for the covert collection of information if disclosure of such information would endanger the performance of the functions of the security authority. Such information shall be classified as secret for 50 years;

3) the classification of budget expenditure and reports on the implementation of the budget of a security authority. Such information shall be classified as secret for 25 years.

(3) Regarding the operation of a security authority in dealing with an emergency, the plan for responding to emergencies, including the methods and tactics used, and the code of conduct for employees participating in responding to the emergency shall be a state secret. Such information shall be classified as confidential for 20 years. Classification shall expire upon the public use of the information in an emergency.

(4) With respect to information covertly collected upon the performance of the tasks of a security authority and the information concerning the collection thereof, the following shall be a state secret:

1) information which has been and is being covertly collected based on the Security Authorities Act, and the plans and instructions for collection thereof. Such information shall be classified as secret for 25 years. Classification expires if, according to a decision of the director general of the security authority, the public use of such information is necessary for the performance of the functions of the security authority. This clause does not apply to the

logs automatically saved in the equipment of an electronic communications operator or a processor of personal data;

2) the information specified in clause (1) if the disclosure thereof would endanger the life or health of a person or the protection of information classified as top secret. Such information shall be classified as top secret for 50 years;

3) the methodology and tactics of collection of the information specified in clause (1). Such information shall be classified as secret for 50 years;

4) information concerning the methods and sources of signals intelligence. Such information shall be classified as top secret for 25 years;

5) Reports containing lists of activities for the covert collection of data based on the Security Authorities Act which do not reflect information classified as top secret. Such information shall be classified as secret for 25 years;

6) Tasks for the collection of information assigned by the Government of the Republic and the Security Committee of the Government of the Republic to a security authority. Such information shall be classified as secret for 25 years;

7) Information which is received by the Security Police Board in the course of covert collection of information based on the Security Authorities Act concerning committed and prepared crimes which do not belong to the investigative jurisdiction of the Security Police Board, provided that such information does not reveal the sources or the tactics of collection of the information or the information specified in clauses 2)-6). Such information shall be classified as restricted for 25 years.

(5) With respect to information analysed and synthesised in the course of performance of the functions of a security authority, the following shall be a state secret:

1) information analysed and synthesised in the course of performance of the functions of a security authority which deals with foreign states, foreign factors or activity. Such information shall be classified as restricted for 15 years;

2) information analysed and synthesised in the course of performance of the functions of a security authority which deals with internal or foreign sources of danger. Such information shall be classified as confidential for 15 years;

3) risk assessments prepared by the security authority. Such information shall be classified as secret for 50 years;

4) Risk assessments prepared by the security authority with the aim of provision of security protection to an event or a person. Such information shall be classified as restricted for 15 years;

5) information analysed and synthesised by the security authority whose source data is classified on a higher level or for a longer period than provided in clauses 1)-4) shall be classified based on the state secret subcategory that prescribes for the highest level and longest term of classification for the source data;

6) information prepared with the aim to prevent danger or damage to the interests of the state by way or informing the public or to inform the public of the activity of a security authority shall not be classified based on clauses 1)-5). The part of information subject to entry in a criminal file shall also not be classified.

(6) With respect to information concerning structural units and staff of security authorities, and their functions, the following shall be a state secret:

1) the structure of a security authority, with the exception of those structural units which are published in the statutes of the corresponding security authority. Such information shall be classified as secret for 25 years;

2) the functions of structural units and employees of a security authority, except for information whose disclosure does not damage the security of the Republic of Estonia. Such information shall be classified as secret for 25 years;

3) the consolidated data concerning the staff of a security authority and the composition of staff performing duties related solely to the covert collection of data. Such information shall be classified as secret for 25 years;

4) information contained in the documents register of a security authority. Such information shall be classified as secret for 25 years, or at a higher level of classification and for a longer term if the register contains information with the corresponding classification level and term.

(7) Information concerning persons who have been recruited for secret co-operation by a security authority, and undercover agents, except for information specified in subsection 6 (2), shall be a state secret. Such information shall be classified as top secret for 75 years.

Classification shall expire if twenty years have passed since the death of such person but not more than fifty years since classification of the information.

(8) Information concerning a person who has submitted a personal confession concerning service in security or intelligence organisations or co-operation therewith to the Security Police Board pursuant to the procedure provided for in clause 5 (2) 1) of the Procedure for Registration and Disclosure of Persons who Have Served in or Co-operated with Intelligence or Counter-intelligence Organisations of Security Organisations or Military Forces of States which Have Occupied Estonia Act, unless the person who was in service in security or

intelligence organisations or co-operated therewith, in relation to such service or co-operation, has committed an offence which, according to the law in force in the Republic of Estonia, is punishable as a criminal offence of the first degree or has committed crimes against humanity or war crimes and the committing of an offence or crime by the person has been proved by court with a judgment which has entered into force, or unless the person who was in service in the security or intelligence organisations or co-operated therewith was the President of the Republic, a member of the Riigikogu or the Government of the Republic, or a justice of the Supreme Court shall be a state secret. Such information shall be classified as secret for 50 years. Classification shall expire if twenty years have passed since the death of such person but not more than fifty years since classification of the information.

(9) With respect to information concerning the coordination of the activities of security authorities, their cooperation with the Defence Forces and information concerning the work of the National Defence Council and the Security Committee of the Government of the Republic, the following shall be a state secret:

- 1) information concerning foreign relations in the area of security prepared by the officials of the State Chancellery engaged in the coordination of work of the security authorities, and the organisation of the work of the Security Committee of the Government of the Republic, unless it contains information specified in clause 2) of this subsection. Such information shall be classified as restricted for 30 years;
- 2) information concerning cooperation with a foreign state or international organisation in the area of security of a structural unit of the State Chancellery engaged in the coordination of work of the security authorities and the organisation of the work of the Security Committee of the Government of the Republic. Such information shall be classified as confidential for fifty years unless agreed otherwise. Such information shall not be classified if it has been made public lawfully;
- 3) information concerning the topics discussed in the meetings of the Security Committee of the Government of the Republic and its sub-committees, except for information published by a decision of the Security Committee of the Government of the Republic with the aim to prevent danger or damage to the interests of the state by way or informing the public or to inform the public of the activity of the Security Committee. Such information shall be classified as restricted for 25 years;
- 4) the duties of a structural unit of the State Chancellery engaged in the coordination of work of the security authorities and the organisation of the work of the Security Committee of the Government of the Republic, and the employees thereof, except for information whose

disclosure does not damage the security of the Republic of Estonia. Such information shall be classified as restricted for 25 years;

5) risk assessments and the list of national priorities for the collection of information prepared by a structural unit of the State Chancellery engaged in the coordination of work of the security authorities and the organisation of the work of the Security Committee of the Government of the Republic. Such information shall be classified as secret for 50 years;

6) information analysed and prepared, based in the information submitted by security authorities, by a structural unit of the State Chancellery engaged in the coordination of work of the security authorities and the organisation of the work of the Security Committee of the Government of the Republic. Such information shall be classified as secret for 50 years;

7) information whose source data is classified at a higher level or for a longer period than provided in clauses 3) and 6) of this subsection shall be classified based on the state secret subcategory that prescribes for the highest level and longest term of classification for the source data.

(10) With respect to information concerning the persons and bodies simulated and shadow information used by security authorities, the information which demonstrates the connection of the bodies simulated and shadow information used with the security authority shall be a state secret. Such information shall be classified as secret for 50 years.

§ 8. Subcategories of state secret regarding infrastructure and data protection

(1) With respect to information concerning the security, intrusion detection, communications and information systems of the Office of the President of the Republic, the State Chancellery, security authorities, the Ministry of Defence, the Defence Forces, the National Defence League, the Defence Resources Agency and the Ministry of Foreign Affairs, including foreign missions, the following shall be a state secret:

1) consolidated information concerning the electronic access, intrusion detection or video surveillance systems of the Office of the President of the Republic, the State Chancellery, security authorities, the Ministry of Defence, the Defence Forces, the National Defence League, the Defence Resources Agency and the Ministry of Foreign Affairs, including foreign missions, to the extent of one building or a part of a building considered to be an integral whole, which contains data concerning the location, type, make or model of the equipment which constitute a system, the security areas or zones, or a general description of the system. Such information shall be classified as confidential for 30 years;

- 2) analyses and assessments concerning the electronic access, intrusion detection or video surveillance systems of the Office of the President of the Republic, the State Chancellery, security authorities, the Ministry of Defence, the Defence Forces, the National Defence League, the Defence Resources Agency and the Ministry of Foreign Affairs, including foreign missions, which reflect the functioning and efficacy of such systems. Such information shall be classified as restricted for 30 years;
- 3) consolidated information concerning the electronic access, intrusion detection or video surveillance systems of the Office of the President of the Republic, the State Chancellery, security authorities, the Ministry of Defence, the Defence Forces, the National Defence League, the Defence Resources Agency and the Ministry of Foreign Affairs, including foreign missions, to the extent of one building or a part of a building considered to be an integral whole, which contains data concerning the location of the central processing units of such systems. Such information shall be classified as restricted for 30 years;
- 4) consolidated information concerning the electronic access and intrusion detection systems of the Office of the President of the Republic, the Ministry of Defence, the Defence Forces, the National Defence League and the Defence Resources Agency to the extent of one building or a part of a building considered to be an integral whole, which contains data concerning the location and types of the terminal equipment (sensors) of such systems, and the security areas and zones created thereby. Such information shall be classified as restricted for 30 years;
- 5) consolidated information concerning the electronic access and intrusion detection systems of security authorities and the Ministry of Foreign Affairs, including foreign missions, to the extent of one building or a part of a building considered to be an integral whole, which contains data concerning the location and types of the terminal equipment (sensors) of such systems, and the location and status of the security areas and zones, or a security area created thereby. Such information shall be classified as restricted for 30 years;
- 6) information concerning the electronic access and intrusion detection systems of security authorities and the Ministry of Foreign Affairs, including foreign missions, to the extent of one building or a part of a building considered to be an integral whole, which contains data concerning the make, models and other technical particulars of the equipment which constitute such systems. Such information shall be classified as confidential for 30 years;

- 7) the set of information processed by the electronic access or intrusion detection system of security authorities and the Ministry of Foreign Affairs, including foreign missions. Such information shall be classified as restricted for 30 years;
- 8) the set of resetting information of the electronic access or intrusion detection system of the Office of the President of the Republic, the State Chancellery, security authorities, the Ministry of Defence, the Defence Forces, the National Defence League, the Defence Resources Agency and the Ministry of Foreign Affairs, including foreign missions. Such information shall be classified as restricted for 30 years;
- 9) information concerning the video surveillance system of the Ministry of Foreign Affairs, including foreign missions to the extent of one building or a part of a building considered to be an integral whole, which contains data concerning the equipment constituting such system and the make and models thereof. Such information shall be classified as restricted for 30 years;
- 10) consolidated information concerning the video surveillance systems of security authorities, the Ministry of Defence, the Defence Forces, the National Defence League, the Defence Resources Agency and the Ministry of Foreign Affairs, including foreign missions, to the extent of one building or a part of a building considered to be an integral whole which contains data concerning the location of the central processing units used in such systems. Such information shall be classified as restricted for 30 years;
- 11) the set of resetting information of the video surveillance systems of security authorities, the Ministry of Defence, the Defence Forces, the National Defence League, the Defence Resources Agency and the Ministry of Foreign Affairs, including foreign missions. Such information shall be classified as restricted for 30 years;
- 12) consolidated information concerning the automatic fire alarm systems of security authorities, the Ministry of Defence, the Defence Forces, the National Defence League, the Defence Resources Agency and the Ministry of Foreign Affairs, including foreign missions, to the extent of one building or a part of a building considered to be an integral whole, which contains data concerning the location, type, make, models of the equipment which constitute such systems, the connections between the equipment and a general description of the system. Such information shall be classified as restricted for 30 years;
- 13) information concerning the video surveillance systems and automatic fire alarm systems of security authorities, the Ministry of Defence, the Defence Forces, the National Defence League, the Defence Resources Agency and the Ministry of Foreign Affairs, including foreign missions which reflects the connections between such systems and utility

systems located in the same building or part of building. Such information shall be classified as restricted for 30 years;

14) the analyses and assessments concerning the physical security measures of the Office of the President of the Republic, the State Chancellery, security authorities, the Ministry of Defence, the Defence Forces, the National Defence League and the Defence Resources Agency which reflect the functioning and efficacy of the security measures. Such information shall be classified as confidential for 30 years;

15) information concerning the radio frequencies permanently used for signals intelligence, air surveillance, marine surveillance, security and guarding of objects and military direction during war-time, emergency situations and states of emergency. Such information shall be classified as confidential for 30 years;

16) information concerning lists of data concerning national communications networks and information systems of the Defence Forces. Such information shall be classified as confidential for 30 years;

17) information concerning the communications plan and communications scheme of the defence districts of the Defence Force and the lists of data pertaining thereto. Such information shall be classified as restricted for 10 years;

18) information concerning the structure, security methods, security means and special software of the communications and information systems processing data intended for the internal use of the Defence Forces and the National Defence League, except for classified information. Such information shall be classified as restricted for 10 years or until the restriction on access to such data expires;

19) information concerning the structure of war-time communications systems of the Defence Forces, and related protective equipment. Such information shall be classified as confidential for 25 years;

20) information concerning the description of the crypto device used in the communications system of the air surveillance system of the air forces. Such information shall be classified as confidential for 10 years;

21) information concerning the description of a unkeyed crypto device used in the communications system of the air surveillance system of the air forces. Such information shall be classified as confidential for 10 years;

22) information concerning the description of a keyed crypto device used in the communications system of the air surveillance system of the air forces. Such information shall be classified as secret for 10 years;

23) information concerning the schemes of the communications links used in the communications system of the air surveillance system of the air forces. Such information shall be classified as confidential for 10 years;

24) information concerning the parameters and operational capacity of the data transmission equipment of the air surveillance systems. Such information shall be classified as confidential for 10 years;

25) information concerning the logical architecture of the communications and information systems of the Ministry of Foreign affairs and foreign missions, including the cabling of the networks to the extent of one building or a part of a building considered to be an integral whole. Such information shall be classified as confidential for 30 years or until the network is transferred or its use is terminated.

26) information concerning the methods and means used by the Information Board for organising and control of special telecommunications. Such information shall be classified as confidential for 30 years.

(2) With respect to information concerning the processing systems for state secrets and classified information of foreign states, the following shall be a state secret:

1) requirements established by the Minister of Defence for cryptomaterial, and the processing and protection thereof. Such information shall be classified as restricted for 30 years;

2) Requirements for ensuring radiation safety established by the Minister of Defence. Such information shall be classified as restricted for 30 years;

3) results of measuring radiation safety in the premises of the location of the processing system. Such information shall be classified as confidential for 25 years;

4) data contained in the register or sub-register of cryptomaterial. Such information shall be classified as confidential for 25 years;

5) the source codes specially created for persons in possession of classified information for processing of classified information. Such information shall be classified as restricted for 30 years;

6) information concerning the technical data and security measures pertaining to a processing system processing information classified as restricted. Such information shall be classified as restricted for 30 years;

7) the conditions for processing information by a processing system for information classified as confidential or a higher level of classification, and the division of tasks between

the users upon processing of classified information. Such information shall be classified as restricted for 30 years;

8) information concerning the technical data and security measures pertaining to a processing system processing information classified as confidential. Such information shall be classified as confidential for 30 years;

9) information concerning the technical data and security measures pertaining to a processing system processing information classified as secret. Such information shall be classified as secret for 50 years;

10) information concerning the technical data and security measures pertaining to a processing system processing information classified as top secret. Such information shall be classified as top secret for 50 years.

(3) The information concerning the technical data and security measures pertaining to a processing system specified in clauses (2) 6) and 8)-10) shall mean information which sets out:

1) results of measuring the radiation safety of the equipment of the processing system unless such results have been disclosed by the manufacturer;

2) the technical specification of the processing system;

3) network scheme of the processing system;

4) technical information concerning connection of the processing system with another information processing system and information concerning applied security measures;

5) settings of the software for administration of the electronic crypting keys within the processing system;

6) security measures to be applied in compensation of failure to comply with an electronic data security requirement provided by legislation;

7) results of the risk analysis of the processing system;

8) estimated residual risks of the processing system;

9) results of the vulnerability analysis of the processing system.

(4) With respect to information concerning the buildings and construction works in the use of a structural unit of the Defence Forces which deals with intelligence and counter-intelligence, the information concerning the plans of the buildings, premises adjusted for special needs such as storage facilities, premises housing information technology and telecommunications equipment, peripheral structures and general communications used by a structural unit of the Defence Forces which deals with intelligence and counter-intelligence shall be a state secret. Such information shall be classified as confidential for 50 years or until

the corresponding construction works is transferred or its intended purpose changes, provided that declassification has been prescribed by a decision.

(5) With respect to information concerning the storage facilities for weapons and munitions of war of the Defence Forces and the National Defence League, the following shall be a state secret:

- 1) information concerning special requirements for guaranteeing the safety of the storage facilities for ammunitions or munitions, except for the requirements established for security and intrusion detection systems. Such information shall be classified as restricted for 10 years or until the end of the possession of the storage facility for ammunitions or munitions;
- 2) the set of information pertaining to the storage facilities for ammunitions or munitions of the Defence Forces or the National Defence league. Such information shall be classified as restricted for 20 years.

(6) With respect to evacuation of classified media of possessors of information, the information regarding the evacuation of the media containing information classified as confidential or a higher level of classification shall be a state secret. Such information shall be classified as confidential for 20 years.

(7) With respect to information concerning the security and intrusion detection systems of security areas of possessors of information, the information concerning the plans and schemes pertaining to the intrusion detection systems installed within the security areas of the holders of classified information and the lists of equipment used in the system and located in the security areas shall be a state secret. If the system installed within a security area is a part of a larger intrusion detection system, only the plans, schemes and lists pertaining to the equipment located within the security area shall be classified. Such information shall be classified as confidential until the end of using the premises as a security area but not longer than for 30 years.

Chapter 3

Declassification, Change of Basis, Level and Term for Classification of State Secret

Division 1

Premature Declassification of State Secret

§ 9. Application for premature declassification

- (1) An agency or constitutional institution who has no competence to declassify a state secret created thereby before the expiry of the term shall submit, in the case provided in subsection 13 (4) of the State Secrets and Classified Information of Foreign States Act, an application for the premature declassification of the state secret to the Government of the Republic through the minister into whose area of government it belongs. If the agency or constitutional institution does not belong in the area of government of any ministry, it shall submit the application to the Government of the Republic through the Minister of the Interior.
- (2) The application shall set forth the reasons for the need for premature classification, the agency or constitutional institution to whom such information has been forwarded, and specify whether, after declassification, such information will become information intended for internal use. Any objections submitted to the application shall be appended to the application. In the case of information specified in subsection 13 (2) of the State Secrets and Classified Information of Foreign States Act, the written consent of the person shall also be appended to the application.
- (3) A minister has the right to send the application to the Security Committee of the Government of Republic to obtain its opinion.

§ 10. Submission of objections to application

- (1) Before application for declassification, the agency or constitutional institution specified in subsection 9 (1) shall inform all the agencies and constitutional institutions to whom a medium containing the state secret has been forwarded of the intention to submit such application, and shall grant them a term of at least one month for submission of objections. The agencies and constitutional institutions whose functions such information may concern shall also be given notice as necessary.
- (2) The notice on the intention to prematurely declassify information shall set forth the reasons for the need for premature declassification and specify whether, after declassification, such information will become information intended for internal use.
- (3) An agency or constitutional institution which receives such notice shall submit its objections to the premature declassification of a state secret not later than within the term granted on the basis of subsection (1) of this section.
- (4) Upon submission of the application to the Government of the Republic, the minister shall consider the objections submitted to the application.

§ 11. Notification of intention to declassify by agency competent to declassify

(1) An agency or constitutional institution who is competent to declassify a state secret created thereby before the expiry of the term shall inform all the agencies and constitutional institutions to whom a medium containing the state secret has been forwarded of the intention to submit such application, and shall grant them a term of at least one month for submission of objections. The agencies and constitutional institutions whose functions such information may concern shall also be given notice as necessary.

(2) A notice on the intention to declassify shall set forth the reasons for premature declassification, the planned date of declassification and an explanation whether, after declassification, such information will become information intended for internal use.

(3) An agency or constitutional institution which receives such notice shall submit its objections to the premature declassification within the term granted on the basis of subsection (1) of this section.

(4) Upon deciding on premature declassification, the head of the agency or constitutional institution specified in subsection (1) shall consider the objections by agencies and constitutional institutions.

§ 12. Notification of agencies and constitutional institutions specified in subsection 35 (3) of the State Secrets and Classified Information of Foreign States Act of premature declassification

If an agency or constitutional institution who has received a notice specified in §§ 10 and 11 has forwarded the said state secret to the agency or constitutional institution specified in subsection 35 (3) of the State Secrets and Classified Information of Foreign States Act, is shall notify such agency or constitutional institution of having received the notice on the intention to prematurely classify a state secret. An agency or constitutional institution notified in this manner has the right to submit its objections pursuant to the same procedure and during the term granted by the agency or constitutional institution intending to submit an application for the premature declassification or to prematurely declassify information.

§ 13. Notification of premature declassification

(1) If an agency or constitutional institution declassifies a state secret created thereby before the expiry of the term, it shall immediately give notice thereof to all units in possession of a medium containing such state secret.

(2) If the Government of the Republic declassifies a state secret before the expiry of the term based on an application submitted or forwarded by a minister, the minister shall

immediately give notice of the declassification of the state secret to all agencies and constitutional institutions to whom a medium containing such state secret has been forwarded.

(3) An agency or constitutional institution who has forwarded a declassified medium to an agency or constitutional institution specified in subsection 35 (3) of the State Secrets and Classified Information of Foreign States Act, shall also immediately inform such agency or constitutional institution of the declassification.

Division 2

Extension of Term of Classification of State Secret

§ 14. Application for extension of term of classification

(1) An agency or constitutional institution who has no competence to extend the term of classification of a state secret created thereby shall submit an application for the extension of the term of classification to the Government of the Republic through the minister into whose area of government it belongs. If the agency or constitutional institution does not belong in the area of government of any ministry, it shall submit the application to the Government of the Republic through the Minister of the Interior.

(2) An application for extension of the term of classification of information classified as state secret shall be submitted to the Government of the Republic, if possible, at least three months prior to the expiry of the term of classification.

(3) The application shall set forth the reasons for the need to extend the term of classification and specify the agencies and constitutional institutions to which such information has been forwarded. Any objections to the application shall be appended to the application.

(4) A minister has the right to send the application to the Security Committee of the Government of Republic to obtain its opinion.

§ 15. Submission of objections to extension of term of classification

(1) Before application for extension of the term for classification, the agency or constitutional institution specified in subsection 14 (1) shall inform all the agencies and constitutional institutions to whom media containing the state secret has been forwarded of the intention to submit such application, and shall grant them a term of at least one month for responding.

(2) A notice on intention to extend the term for classification shall set forth the reasons for extension of the term for classification .

(3) An agency or constitutional institution which receives such notice shall submit its objections to the extension of the term of classification within the term granted on the basis of subsection (1) of this section.

(4) Upon submission of the application to the Government of the Republic, the minister shall consider the objections submitted to the application.

§ 16. Notification of extension of term of classification

(1) If an agency or constitutional institution has extended the term of classification of a state secret created thereby, it shall immediately give notice thereof to all units in possession of a medium containing such state secret.

(2) If the Government of the Republic extends the term of classification of a state secret based on an application submitted or forwarded by a minister, the minister shall immediately give notice of the extension of the term of classification to all agencies and constitutional institutions to whom a medium containing such state secret has been forwarded.

(3) An agency or constitutional institution who has forwarded a classified medium whose term of classification has been extended to an agency or constitutional institution specified in subsection 35 (3) of the State Secrets and Classified Information of Foreign States Act, shall also immediately inform such agency or constitutional institution of the extension of classification.

Division 3

Correction of Classification Data

§ 17. Submission of application for correction of classification data

(1) An agency or constitutional institution whose employee or public servant has no competence to correct classification data shall submit, in the case provided by subsection 15 (1) of the State Secrets and Classified Information of Foreign States Act, an application for the correction of classification data to the Government of the Republic or the Minister of the Interior through the minister to whose area of government it belongs. A person holding a processing permit shall submit the application through the agency which supported the grant of permit for processing state secrets to such person.

(2) The application shall set forth the reasons for correction of classification data and provide an explanation whether such data will thereafter become public information without any restrictions to access, internal information or classified information, specifying the basis and term for classification, and specify the agencies and constitutional institutions to which such data has been forwarded. Any objections to the application shall be appended to the application.

(3) A minister has the right to send the application to the Security Committee of the Government of Republic to hear its opinion.

§ 18. Notification of intention to submit application for correction of classification data

(1) Before submission of an application for the correction of classification data, notice shall be given to all agencies and constitutional institutions to whom media containing the corresponding state secret has been forwarded, and a term of one month shall be granted for responding to such agencies and institutions.

(2) A notice on correction of classification data shall set forth the reasons for correction of the classification data together with an explanation whether such data will thereafter become public information without any restrictions to access, or internal information or classified information, specifying the basis and term for classification.

(3) An agency or constitutional institution which receives such notice shall submit its objections to the correction of the data related to the classification of a state secret not later than within the term granted on the basis of subsection (1) of this section.

(4) Correction of classification data shall be decided based on the application and any objections submitted thereto.

§ 19. Notification of intention to correct classification data related to self-created state secrets

(1) Before correction of classification data related to a state secret created by a processing unit, the processing unit shall notify all the agencies and constitutional institutions to whom media containing the state secret has been forwarded of such intention, and shall grant them a term of at least one month for responding.

(2) The notice shall set forth the reasons for correction of the classification data together with an explanation whether such data will thereafter become public information without any restrictions to access, or internal information or classified information, specifying the basis and term for classification.

(3) An agency or constitutional institution which receives such notice shall submit its objections to the correction of the classification data within the term granted on the basis of subsection (1) of this section.

(4) Upon deciding on the extension of the term of classification, the processing unit specified in subsection (1) shall consider any objections submitted by other agencies and constitutional institutions.

§ 20. Notification of agencies and constitutional institutions specified in subsection 35 (3) of the State Secrets and Classified Information of Foreign States Act of intention to correct classification data

If an agency or constitutional institution who has received the notice specified in §§ 10 and 11 has forwarded the state secret to the agency or institution specified in subsection 35 (3) of the State Secrets and Classified Information of Foreign States Act, it shall notify such agency or constitutional institution of having received the notice on the intention to correct the data related to the classification of a state secret. An agency or constitutional institution notified in this manner has the right to submit, during the term granted for submission of objections to the correction of classification data, its objections pursuant to the same procedure as the agencies and constitutional institutions who have received a notice on the intention to correct classification data.

§ 21. Notification of correction of classification data

(1) If a processing unit corrects classification data, it shall immediately give notice thereof to all the processing units to whom media containing the corresponding state secret has been forwarded.

(2) If correction of classification data has been decided by the Government of the Republic based on an application, the ministry who submitted the application shall inform all the processing units to whom media containing the corresponding state secret has been forwarded.

(3) If classification data is corrected by a resolution in a misdemeanour matter or a court judgment, the Security Police Board shall inform all the processing units to whom media containing the corresponding state secret has been forwarded.

(4) A processing unit who has forwarded a classified medium whose classification data has been corrected to an agency or constitutional institution specified in subsection 35 (3) of

the State Secrets and Classified Information of Foreign States Act, shall immediately inform such agency or constitutional institution of the correction of the classification data.

Chapter 4

Requirements for Organisation of Protection of Classified Information

§ 22. Requirements for guidelines for protection of state secrets of agencies, constitutional institutions and legal persons in possession of state secrets

(1) The guidelines for the protection of state secrets of agencies, constitutional institutions and legal persons in possession of state secrets shall regulate the following issues, taking account of the specific character of the processing unit:

- 1) the procedure for receipt and forwarding of classified media arriving from and to be sent outside;
- 2) procedure for registration of classified media;
- 3) procedure for storage of the key and access code to a safe;
- 4) procedure for handling access permits and access certificates;
- 5) procedure for correction of classification data;
- 6) procedure for holding classified meetings;
- 7) location of the security area;
- 8) guarding of the security area, procedure for entry into, moving within and leaving the security area;
- 9) plan for protection of classified information in emergencies;
- 10) notifying of the persons who have attempted, in any manner, to gain unlawful access to classified information, and notification of violation of the requirements of the State Secrets and Classified Information of Foreign States Act or legislation issued on the basis thereof;
- 11) list of procedures, guidelines and other rules regulating the processing of state secrets in force in the agency, constitutional institution or legal person;
- 12) procedure for and method of destruction of classified media;
- 13) extent of the administrative area;
- 14) procedure for bringing weapons, technical means or other objects that could be used as technical means for wire tapping or recording into the security area;
- 15) procedure for notification of the loss, doubt of loss or other loss of possession of entry permits or means granting entry;

16) appointment of a person with whom spare keys of the lock and lock codes for the safe used to store media classified as confidential or on a higher level of classification shall be deposited for safekeeping.

(2) In addition to the issues specified in subsection (1), the guidelines for the protection of state secrets may provide, for example:

- 1) the procedure for the receipt and forwarding of classified media within the processing unit (within the limits of the security area, through the administrative area);
- 2) a specific procedure for forwarding classified media;
- 3) procedure for reproduction of classified media;
- 4) procedure for inspection rounds by the local manned guard;
- 5) specifics of the entry permits of persons who have the right to independently enter the security area, to be specified for the persons who work at the same processing unit;
- 6) specifics for allowing visitors to enter the security area, to be specified for persons who work at the same processing unit;
- 7) establishment of guidelines for the application of safety requirements for processing systems of state secrets.

(3) The part of the guidelines for the protection of state secrets which must be classified shall be established as an annex to the guidelines or as a separate document.

§ 23. Requirements for activity of persons or structural units organising protection of state secrets in agencies, constitutional institutions and legal persons in possession of state secrets
A person or structural unit organising the protection of state secrets in an agency, constitutional institution or legal persons in possession of state secrets shall:

- 1) organise the protection of state secrets and adherence to the requirements of the State Secrets and Classified Information of Foreign States Act and legislation issued on the basis thereof;
- 2) advise employees in the processing of classified information;
- 3) organise the training of persons with the right of access in issues of protection of classified information, including in the area of electronic information security;
- 4) organise the work of guards who are guarding security areas and supervise their activities unless such duty is assigned to another official;
- 5) verify the formal conformity of applications for clearances, confirmations, access permits and processing permits, applications for the extension thereof, and of forms to be

filled out by applicants for access permits and processing permits before forwarding such documents;

- 6) keep record of the permits and certificates for access to state secrets held by the employees;
- 7) maintain a record of classified media;
- 8) keep a list of persons who use safes;
- 9) communicate information to the Security Police Board or the Headquarters of the Defence Forces or the Information Board, as appropriate, at least every ninety days on the appointment of persons who do not hold access permits to positions where access to state secrets classified as restricted is required, on the release of persons from such positions and on any decision to grant permission to access state secrets classified as restricted to persons outside the service;
- 10) organise adherence to the requirements of electronic information security and communicate corresponding information to the Information Board at the request thereof;
- 11) document information concerning data processing systems and parts thereof pursuant to the guidelines for application of security requirements;
- 12) develop the Security Operation Procedures in co-operation with the system or network administrators and ensure the introduction and availability thereof;
- 13) appoint the persons who have the right to access the processing system or a part thereof, and determine the content and extent of the right of access unless it has been established by the head of the processing unit;
- 14) issue passwords and other physical and electronic means which grant access to information and ensure the periodic changing and keeping records of such means;
- 15) monitor and document the maintenance and repair of processing systems and the modification of the configurations thereof;
- 16) maintain records of the parts of the processing system which contain classified information, including floppy discs and other removable storage media and the users thereof and periodically verify the actual existence, content, storage conditions and marking of the storage media;
- 17) ascertain the circumstances of non-occurrence of an event or process or the unauthorised use of the processing system;
- 18) immediately inform the Security Police Board and correspondingly, the Information Board, the General Staff of the Defence Forces or the authorised representative of national security of becoming aware of a violation of the requirements of the State Secrets and

Classified Information of Foreign States Act or legislation issued on the basis thereof, or of disclosure of classified information to a person who has no right to access information of the corresponding level of classification;

19) collect explanations from persons who have violated the requirements of the State Secrets and Classified Information of Foreign States Act or legislation issued on the basis thereof.

Chapter 5

Requirements for Processing Classified Information and Classified Media

Division 1

Security Areas

Subdivision 1

General Requirements for Security Areas

§ 24. General requirements for security areas

- (1) A security area shall have a clearly defined and protected perimeter, and the possibility to monitor all entrances and exits, and a system for monitoring entry into and exit from the security area which guarantees that only persons with the requisite level of right of access can independently enter the security area.
- (2) The use of an area as a security area shall be approved beforehand by the Security Police Board, the Headquarters of the Defence Forces or the Information Board correspondingly.
- (3) The Security Police Board, the Headquarters of the Defence Forces or the Information Board may make an exception in the requirements for security areas provided by this Regulation with respect to a specific building or processing unit if application of the requirements is not technically possible or is impossible due to reasons arising from law, or if the conformity of the security area can be guaranteed by other means.
- (4) The general requirements for security areas shall apply to temporary and mobile security areas unless otherwise provided by this Regulation.
- (5) Upon termination of the use of an area as a security area, the authority which granted its approval for such use shall be informed thereof within thirty days after the end of the use.

§ 25. Location of security area

- (1) A security area shall be located in premises which are in the direct possession of the processing unit in possession of a state secret. Information may be processed outside of a security area in the direct possession of a processing unit only within the security area of a processing unit which has the need and right to access the specific information.
- (2) Before starting to plan for the erection of a security area, the representatives of the authority competent to grant approval shall be consulted in order to determine the best possible location for a security area in the building.
- (3) Where possible, a security area should not be erected on the first or last floor of a building.
- (4) Where possible, the location of a security area in a building shall be selected such that any windows would face a territory in the possession of the agency processing the state secrets.
- (5) Persons and structural units which process state secrets or classified media should, if possible, be situated in a close proximity of each other, for example in one and the same room or one and the same wing of a building in the agency.

§ 26. Mobile and temporary security area

- (1) As an exception, a security area may also be erected on moving platforms (hereinafter mobile security area) or areas which are not usually used as security areas (hereinafter temporary security area). A vehicle, trailer, bunker, container, caravan, tent, or other construction works suitable for such function may be used as mobile or temporary security areas. Where possible, fixed structures should be used for a temporary security area.
- (2) The use of such security area shall be approved beforehand by the Security Police Board, the Headquarters of the Defence Forces, or the Information Board correspondingly, and also by the authorised representative of national security if classified information of foreign states is processed in the security area. An agency seeking approval for a mobile or temporary security area shall submit, for obtaining such approval, a written application to the approving authority at least thirty days before commencing the use of such security area.
- (3) In case of urgency, the term specified in subsection (2) may be reduced with the consent of the approving authority.
- (4) Where possible, all the requirements for security areas shall be applied to mobile and temporary security areas and, if this is not possible, the security of classified information shall be guaranteed by other means.

(5) By way of exception, mobile and temporary security areas may be established based on an oral order of the head of the agency in possession of a state secret in the case of an emergency situation, a state of emergency, mobilisation or a state of war. An order given orally shall be recorded in writing as soon as possible. Agencies whose activities require the establishment of mobile or temporary security areas under such circumstances shall provide information to this effect in the crisis management plans of the agencies themselves as well as the plans of other levels, such as counties and ministries, and inform the approving agency thereof.

(6) Only the classified media needed for the performance of a particular task shall be processed within a mobile or temporary security area. The classified media shall be moved to a permanent security area immediately after the need for processing has ended.

(7) In choosing a location for a mobile or temporary security area, the possibility to effectively and safely perform the task shall be the first priority.

(8) The head of an agency shall appoint a person who shall be responsible for the security measures to be applied for the protection of classified media within a mobile or temporary security area (hereinafter responsible person).

(9) If discrepancies from the data submitted for approval become evident upon use of a security area, the responsible person shall notify the approving authority thereof in writing no later than within thirty days after such change took place.

§ 27. Walls, ceiling and floor of security area

(1) The walls, ceiling and floor of a security area shall be made of concrete, steel or stone such that the details of which the walls, ceiling or floor consists could not be easily removed from outside.

(2) A wall between two security areas or an internal wall within a security area may be a lighter structure. The outer walls, ceiling or floor of a security area may be a lighter structure if a permanent manned guard is present in the building or if they have been strengthened by adding physical barriers or technical security equipment.

(3) A security area must be sound-proofed to the extent where sounds originating from such area would not be heard in the neighbouring premises.

§ 28. Door of security area

- (1) The door at the perimeter of a security area (hereinafter door to security area) must be, in the opinion of the approving authority, be sufficiently secure to allow the security guards to react to attempted intrusion before the intruder has crossed the physical barriers.
- (2) The door to a security area shall be fastened to the doorjamb by at least three hinges and the door, at the side of the hinges, shall be fitted with security tenons which withdraw inside the doorjamb when the door closes. The door of a security area shall have an automatic latch which makes the door close automatically after a certain period of time and a sensor which signals that the door has been open for longer than permitted.
- (3) If a conforming door to the security area cannot be installed, the door of the security area shall be guarded by additional security and intrusion detection system equipment.
- (4) The door of a security area shall be fitted with at least two locks one of which must lock automatically, and with at least one mechanical security lock. The tumbler of the security lock must be protected.
- (5) It must not be possible to open the mechanical locks of the security area with a key with which other locks in the building can be opened. If this requirement cannot be fulfilled, the keys must be stored under the same conditions with the keys to a safe.

§ 29. Window of security area

- (1) A security area window located at an easily accessible place like a roof, terrace or extension shall be fitted with anti-burglar security elements. Where necessary, other physical barriers or security and intrusion detection system equipment shall be used to increase the safety of a window.
- (2) The windows of a security area shall be covered with a curtain or opaque film in order to render the inside of the security area invisible.

§ 30. Other openings of security area

Other openings located in a security area shall be protected by physical barriers or security and intrusion detection system equipment to prevent the unlawful installation of technical equipment in the security area or other danger to the information contained in the classified media stored within the security area.

§ 31. Open storage area

The outer walls, ceiling or floor of an open storage area must not be a light structure.

§ 32. Structural protection of mobile and temporary security areas

- (1) A mobile or temporary security area shall have a perimeter clearly defined and protected by a physical barrier which allows control over all entries and exits. At the demand of the approving authority, the location of the security area shall be changed, the structure of the security area shall be strengthened and additional barriers shall be used.
- (2) The structure of a mobile or temporary security area shall guarantee that access or danger to classified information from outside of the security area is precluded.

§ 33. Evacuation plan

- (1) A plan for evacuation of classified media in the case of emergencies shall be prepared with respect to a security area.
- (2) The evacuation plan shall set out all possible emergencies in the case of which classified media must be evacuated or destroyed.
- (3) For every emergency defined based on subsection (2), the course of evacuation or destruction, the persons who have the right to give the corresponding order, the persons to carry out such order, the means for carrying out such order and the place where the classified media shall be evacuated shall be specified.

Subdivision 2

Requirements for Guarding Security Areas

§ 34. General requirements for guarding security areas

- (1) A security area shall be equipped with an intrusion detection system (hereinafter detection system) and have a manned guard on site.
- (2) The requirement for the presence of a manned guard on site does not apply if the electronic security equipment and measures for physical protection allow the manned guard to react to attempted intrusion before the intruder has crossed the physical barriers.
- (3) At times when a security area or a part thereof is empty of persons, it must be placed under surveillance.

§ 35. Requirements for electronic security systems

- (1) An electronic security system shall:
 - 1) send an alarm signal in the case of an intrusion or attempted intrusion;
 - 2) allow the manned guard to react before the intruder has crossed the physical barriers;

- 3) allow the surveillance of the security area to be switched on and off separately and later, to electronically establish the time of switching on and off, and the time of when the alarm signal was sent. Data reflecting such acts shall be preserved for at least one year;
- 4) establish the failures in the system automatically.
- (2) In the case of a failure of the electronic security system, the system shall immediately send an alarm signal to the manned guard.
- (3) The alternate power supply of an electronic security system used for the protection of state secrets shall guarantee the functioning of the system in case of the failure of the main power supply system until the time the security area is placed under manned guard.

§ 36. Manned guard of mobile and temporary security areas

- (1) A mobile or temporary security area shall be protected by mobile or stationary armed guards who shall monitor the whole protected area. Exceptions to such requirement may be made only with the permission of the approving authority based on the risk assessment of the location of the security area. Security guards as well as instructed persons who work within the security area on a twenty-four hour basis may be used for guarding a security area.
- (2) If it is not possible to ensure continuous manning of a mobile or temporary security area, it shall be equipped with an intrusion detection system to send an alarm signal to instructed persons, that is, to the security guards or employers of the security area who must be able to reach the security area within the prescribed reaction time approved by the approving agency. The reaction time shall not be longer than the time during which an intruder is able to cross the physical barriers.

§ 37. Patrolling of on-site manned guards

- (1) On-site security guards shall patrol outside working hours, on days off and on public holidays at different intervals. The interval between patrols shall not exceed two hours unless security cameras are used.
- (2) On-site manned guards shall check all the persons working within the security area and their workplaces. During each subsequent patrol, the rooms where persons were working during the previous patrol shall be checked.
- (3) During subsequent patrols, on-site manned guards shall check all rooms over the course of three patrols and the rooms to be checked during each patrol shall be chosen at random. The patrols shall also make sure that there are no signs of intruders in the security

area being patrolled and that all doors, windows and other means of entry to the security area on the route of the patrol are closed and intact.

(4) Based on the right for access and the need to know, the head of a processing unit may restrict the access of manned guards to the security area or a part thereof.

§ 38. Right of on-site manned guards to access state secrets

On-site manned guards patrolling a security area shall have permission to access state secrets at least of the level of classification of the state secrets which are processed within the security area.

Subdivision 3

Presence and Working of Persons in Security Areas

§ 39. Presence of persons in security area

The procedure for presence of persons in a security area shall take account of the right of access and need to know of persons, and shall specify the entry to and exit from the security area by persons.

§ 40. Access of persons with independent right of access to security area

(1) A person who has an independent right of access to a security area shall be issued an entry permit which shall set out the number of the permit. An entry permit need not be issued if the security area consists of only one or two rooms.

(2) A processing unit shall keep record of the entry rights, means of entry and entry permits of persons with the right to access the security area.

(3) A person who works at a security area shall carry an entry permit in a visible manner in order to enable him or her to be identified. The requirement to carry an entry permit in a visible manner does not apply to security authorities. An entry permit shall not be carried in a visible manner outside a security area or administrative area.

(4) The procedure for entry to and exit from a security area shall ensure the identification of persons with an independent right of access upon entry and exit.

(5) In the case of loss, suspected loss or loss of other possession of an entry permit or an object ensuring entry, notice thereof shall be immediately given to the duly appointed person of the processing unit who shall take measures for preventing the use of the entry permit or object ensuring entry.

§ 41. Presence of visitors in security area

- (1) A visitor may be permitted to a security area pursuant to the procedure provided by the guidelines for the protection of state secrets of the processing unit.
- (2) A visitor is issued a numbered visitor's permit which shall bear the word *KÜLALINE* [visitor] and enables the identification of the person who received the permit. A visitor shall carry the visitor's permit in a visible manner.
- (3) An visitor's permit need not be issued if the security area consists of only one or two rooms.
- (4) The issue and return of a visitor's permit, the time the visitor arrived and left, the visitor's given name and surname shall be registered. Identification of a visitor shall take place on the basis of valid identity document.
- (5) A visitor may move within a security area only together with the person who receives the visitor or with the person assigned to escort the visitor. It is prohibited to leave a visitor alone in a security area unless he or she has right of access to the corresponding classification of state secrets which are processed in the security area, considering the principle of need to know.

§ 42. Requirements for working in mobile and temporary security areas

- (1) In the case of removals, the person responsible for a temporary security area shall review the abandoned security area and make sure that no classified media remain in the area.
- (2) After work is finished in a temporary security area, classified media shall be transferred to the permanent security area of the agency for comparison of data and destruction of the materials which have fulfilled their purpose.
- (3) Measures of physical security existing within a temporary security area shall be strengthened as necessary also after the use of the security area has been approved.

Subdivision 4

Requirements for Conduct of Meetings on Classified Information

§ 43. General requirements for conduct of meetings

In order to organise a discussion, meeting, conference, etc. (hereinafter meeting), the following requirements shall be fulfilled:

- 1) the person organising a meeting on classified information shall guarantee that only persons who have the right to access the information to be discussed at the meeting and a need to know such information can access the meeting;
- 2) that which takes place within the meeting room cannot be heard or seen from outside.

§ 44. Holding of meetings within security areas and administrative areas

- (1) The premises used for holding meetings shall be located within a security area or administrative area.
- (2) Rooms which are used for the conduct of a meeting on state secrets classified as restricted may also be located in an administrative area and the requirements provided in this subdivision need not apply to the rooms.

§ 45. Periodic checking of meeting rooms

Meeting rooms shall be periodically checked in order to prevent prohibited audio or video recording. No technical equipment or object which has not undergone prior checks or which could be used for wire tapping or prohibited recording shall not be present in a meeting room during a meeting.

§ 46. Registration of notes made at meeting

The organiser of a meeting shall review all notes and summaries made by the participants at a meeting and other such material, and shall return or forward them to the participants only after the notes containing a state secret have been correspondingly marked and registered.

Division 2

Registration of Classified Media

§ 47. General requirements for registration of classified media

Classified media shall be registered based on the Regulation of the Government of the Republic established based on subsection 58 (1) of the Public Information Act with the exceptions provided in this Regulation.

§ 48. Original documents

In the case a classified document created in several copies, the first original copy is deemed to be the original document. The other documents are deemed to be copies and shall be processed as such.

§ 49. Register of classified media

- (1) All agencies, constitutional institutions and persons in possession of state secrets shall establish registers of classified media (hereinafter registers) for the registration of classified media.
- (2) Depending on the volume of classified media, separate registers may be established for the registration of media classified as top secret, secret, confidential and restricted.
- (3) Media classified as restricted may, with the permission of the head of the processing unit, also be registered in the general document register provided that this does not result in the classified information becoming known to unauthorised persons.
- (4) A sub-register of classified media may be established in each structural unit of an agency by the decision of the head of the processing unit.

§ 50. Requirements for register

- (1) A register of classified media may be maintained on computer or on paper.
- (2) Where possible, a registry entry itself should not contain classified information.
- (3) A processing unit shall ensure the preservation of register data.

§ 51. Data subject to entry in register

- (1) The following shall be entered in the register of classified media:
 - 1) Data necessary for the identification of a medium: registration number, date of registration, date of preparation, the name of the agency who sent the media, registration number of the forwarding agency and for documents, also the name thereof, and the name of the person who prepared and signed the document. Each copy need not be given a new registration number if the consecutive number of the copy is specified;
 - 2) the class of a medium;
 - 3) basis for classification of a media, level of and term for classification, any amendments thereto and the basis for the amendments;
 - 4) the number and consecutive numbers of the copies; the number of copies need not be entered in the register for media classified as restricted or confidential;

- 5) the number of the parts of a medium, and number pages of documents. If a document has been prepared on both sides of a page, the number of pages of such document shall be registered in the register of classified media, with a note that the document has been prepared on both sides of a page;
 - 6) the number of copies; the number of copies need not be entered in the register for media classified as confidential or at a lower level of classification;
 - 7) the name of the processing unit to whom the classified medium or a copy thereof has been forwarded and the time of forwarding; the signature of the recipient or number of the instrument of delivery and receipt;
 - 8) a corresponding notice if the other processing unit has been given permission to forward the information contained in the classified medium to a third processing unit;
 - 9) a notice concerning destruction.
- (2) The following shall be entered in a register of classified media concerning removable electronic storage media:
- 1) the type of storage medium - for example a hard drive, diskette, memory stick;
 - 2) registration number;
 - 3) registration date;
 - 4) the highest level of classification of the information contained in the storage medium;
 - 5) the processing unit to which the storage medium was forwarded and the time of forwarding.

§ 52. Registration of classified media

- (1) A classified medium shall be registered on the day of its preparation or arrival.
- (2) Generally, a classified medium shall be entered in the register once. A classified medium registered in the main register need not be registered in the sub-register of the same processing unit.
- (3) If a set of classified media also contains unclassified media, the unclassified media belonging to the set may be registered in the register of classified media. If a set consists of classified documents which are used separately, then each document which constitutes a part of the set may be registered separately.

§ 53. Registrar

The person who makes entries in the register (hereinafter registrar) shall have right of access which corresponds to the highest classification of the media to be registered. The registrar or

registrars and, where necessary, their substitutes shall be appointed by the head of the processing unit.

§ 54. Registration sheet

- (1) In the case of examination of information contained in a medium classified as secret or at a higher level of classification, a corresponding notice shall be made and the person to examine the media shall give his or her signature to such effect on the registration sheet annexed to the medium or on the medium itself.
- (2) Registration sheets shall be preserved for the same period of time as the register data.

Division 3

Marking of Classified Media

Subdivision 1

General Requirements for Marking

§ 55. Marking of classified media containing state secret

- (1) In cases where marking does not endanger the classification of a state secret, the classified medium shall be marked with a clearly visible classification marking "top secret", "secret", "confidential" or "restricted":
 - 1) printed in double-spaced bold capital letters of at least size 16, or
 - 2) by a clip-mark, sticker or other such manner, printed in red colour, the same size and same form.
- (2) If a medium cannot be marked due to its size, the marking may be made on a label attached to the medium. In small media and justified cases, the marking may be made smaller than provided in clause (1) 1) provided that the marking is clearly visible and legible.
- (3) The basis for classification of information shall be entered on a classified medium containing a state secret in the following form: "State secret pursuant to ...". A reference to this Regulation, the corresponding section, subsection and clause shall be entered in the gap. If a classified medium has been classified on several bases, all such bases shall be entered in the medium.
- (4) The date, number and term of classification of the medium shall also be entered on a classified medium.

(5) The general classification of medium shall correspond to the highest classification of any of its separate parts.

(6) If a medium containing a state secret is to be forwarded to a foreign state or an international organisation, classification markings corresponding to the requirements of the international agreement shall be made on the medium and a notation in English shall be made on the front page stating that the information contained in the medium belongs to the Republic of Estonia.

§ 56. Marking of media containing classified information of foreign states

Media containing classified information of foreign states and parts thereof containing classified information of foreign states shall be marked with the level of classification of the issuer of the classified information of foreign states provided that this is prescribed by an international agreement, and the marking indicating the corresponding level of state secret. The upper right corner of the front page of the media shall be additionally marked with the words "*salastatud välisteave*" [classified information of foreign states] in capital letters together with the name of the originator of the classified information of foreign states, the level of classification and the term for classification if the term for classification has been prescribed by the originator of the foreign information.

§ 57. Marking of copies of and extracts from classified media

(1) A copy shall be marked with the word "*KOOPIA*" [copy]. If the notations entered on a document are not automatically transferred to a copy upon reproduction, the copy shall be marked in the same manner as the original document.

(2) An extract shall be marked with the word "*VÄLJAVÕTE*" [extract], together with the name of original document of which the extract was made and the classification markings of the original document.

§ 58. Additional markings concerning security measures and persons with right of access

(1) If a medium is marked with an additional mark concerning additional security measures or a group of persons with the right to access the medium, a corresponding notation shall be made next to the notation concerning the basis for classification.

(2) Classified cryptomaterials shall be additionally marked by the word "*KRÜPTO*" [crypto].

§ 59. Additional classification markings for packaged media

- (1) If a classified medium or set of data is stored in package, is rolled up, placed in a container or box, or is stored in any other manner where the packaging covers the classification marking, then additional classification markings shall be made on the medium or the packaging such that the fact that this is a medium containing a state secret can be established regardless of whether the medium is packed up or unpacked, and also upon processing the medium.
- (2) The provisions of division 7 of this Chapter apply to packing data media for the purpose of forwarding them.

§ 60. Amendment and deletion of markings

- (1) Classification markings shall be crossed out after expiry of classification upon expiry of the term of classification.
- (2) In the case of premature declassification, the classification marking shall be crossed out and the words "*Salastatus kustutatud ... alusel*" [Declassified based on ...] shall be added next to the notation concerning the basis for classification, also indicating the body which made the decision, the requisite data of the decision and the time of entry into force of the decision.
- (3) In the case of extension of the term of classification, the words "*Salastamistähtaeg pikendatud ... alusel*" [Term of classification extended based on ...] shall be entered next to the notation concerning the basis for classification, also indicating the body which made the extension decision, the requisite data of the decision and the new term of classification.
- (4) In the case of correction of classification data, the incorrect marking shall be crossed out and below that, the words "*Salastatus parandatud ...*" [Classification corrected ...] shall be entered based on the decision to correct the classification data. The name of the body which made the decision and the requisite information concerning the decision or the title, name and signature of the official who made the decision shall be added to such information.
- (5) New markings to the data specified in subsections (2)-(4) shall be made pursuant to the general procedure.

Subdivision 2

Marking of Documents

§ 61. Application of general requirements for formalising documents

Classified documents shall be prepared and formalised in based on the general requirements for the preparation of documents with the specifications arising from this Regulation.

§ 62. Numbering of pages

The pages of a classified document shall be numbered starting from the first page and the total number of pages shall be marked on each page. If a document has been formalised on both sides of a sheet, the pages shall be correspondingly numbered and marked.

§ 63. Marking of documents

(1) A notation concerning the level and basis of classification, the date of registration of the medium, the number and term of classification shall be made in the upper right corner of the front page of a classified document. All the pages of a document shall be marked, in the centre of the upper and lower margin of the page, with a classification marking corresponding to the highest level of classification of the information contained in that page.

(2) A classified document has, as a whole, the highest level of classification of state secrets of any of its separate parts, concerning which a classification marking shall be made on the first page of the document, as well as the title page, and front and back covers if they exist.

§ 64. Marking of annexes to document

If it is possible to use an annex to a written document without the source document, the annex shall be marked and formalised as a separate document.

§ 65. Marking by text paragraph and illustration

If a medium is additionally marked by text paragraph or illustration, the classification marking shall be made at the beginning of the first row and the end of the last row of the classified paragraph, and before and after the classified illustration. The marking indicating the level of classification of information shall be made in bold capital letters in brackets or parentheses. The marking indicating the level of classification can be abbreviated by writing the first letter of the classification level.

§ 66. Marking upon expiry of classification of information contained in documents and correction of classification data

(1) A notation concerning the expiry of classification, declassification before the prescribed term or extension of the term of classification of a document, or amendment of the basis or term for classification shall be made on the first page of the document in the upper right corner on a separate line next to the marking concerning the basis for classification of the media.

(2) On other pages, the classification marking shall be crossed out in the upper and lower margin of the page in the case of expiry of classification and declassification.

§ 67. Marking of sets of documents

(1) Sets composed of classified documents shall be marked with the marking indicating the highest classification level of state secret.

(2) If a set of documents has been joined together in a file or is stored between covers in another manner, the classification marking shall be made on the upper and lower margins of the front and back cover of the file.

(3) In other cases, the classification marking shall be made in the upper and lower margins of the first page of the first document in the set.

(4) If the front page of a set does not contain a state secret, an additional notation "*Märgistatud riigisaladusena kui kogumi esileht*" [Marked as a state secret as the front page of a set] shall be made in the upper right corner of the document.

Subdivision 3

Marking of Other Media

§ 68. Marking of classified photos, transparencies and slides

In the case of classified photos, transparencies and slides, a classification marking shall be made on every photo, transparency and slide.

§ 69. Marking of audio, film and video recording

In the case of audio, film and video recordings, the marking shall be made on the packaging as well as the medium itself, and shall be made clear by the content of the medium upon use thereof.

Subdivision 4

Marking of Electronic Data

§ 70. Marking of files

- (1) The classification level of a file containing classified information shall be marked in capital letters at the beginning of the file name and if possible, also in the metadata of the file.
- (2) If a file contains a document, then in addition to the file, also the document contained in the file shall be marked in conformity to the requirements for marking documents. In marking documents contained in files, it shall be ensured in the best possible manner, that the classification marking would be permanently visible upon display, projection or other manners of emission for reception of the set of data containing the state secret.

§ 71. Marking of electronic messages

- (1) In the case of electronic messages, the classification marking shall be made in capital letters at the beginning and end of the heading and message body in conformity to the requirements for marking documents.
- (2) The heading of a message need not bear a classification marking if the classified medium annexed to the message is crypted and the uncripted part of the message does not contain a state secret.

Division 4

Storing of Classified Media

Subdivision 1

Requirements for Storage Conditions and Means of Storage

§ 72. Safe

- (1) Media which are classified at confidential or a higher level shall be stored in a safe with a code lock with a burglar resistance of at least corresponding to at least the requirements of class 1 of the standard EVS-EN 1143-1.
- (2) Media classified as restricted shall be stored in a locked container, cabinet or drawer which is protected from access by unauthorised persons.
- (3) A safe where media classified as confidential or at a higher level is stored shall be located within a security area.
- (4) If several persons use one and the same safe, the safe shall be physically divided into parts, based on the need to know. In such case, the safe shall contain separate lockable parts.

(5) With the permission of the approving agency, classified media may be stored within a public storage area. The approving agency shall prescribe the highest permissible level of classification at which information may be processed within such area.

§ 73. Storage of classified media during use

(1) Following removal from a safe or other place of storage, classified media shall be under continuous supervision. If the classified documents are not being used at any given moment, they shall be kept so that an empty page is the uppermost or be covered up.

(2) Upon leaving a room, the classified media shall be locked away in a safe, cabinet or drawer in correspondence to their level of classification.

§ 74. Exceptions to general storage conditions

(1) If it is not possible to meet the requirements for the storage of classified media in a processing unit, the classified media shall be transferred for temporary storage to a state agency where such requirements are met.

(2) An approving agency may allow the use of safes with a lower class of burglar resistance than provided in subsection 72 (1) in mobile and temporary security areas.

(3) In exceptional cases, an approving agency may permit the use of other possibilities for storing classified media, such as storage in a packaged state within the security area of the receiving base or headquarters, in a locked metal box, leather pouch or other such place.

(4) In exceptional cases, media classified as secret or confidential may, with the permission of the head of the agency, be stored in a metal filing cabinet or in a drawer for a short time, for example, until a safe of appropriate measurements is found, provided that the place of storage is situated in a security area and is equipped with at least one security device or a three-number combination lock.

Subdivision 2

Protection of Keys and Lock Codes

§ 75. Lock codes of safes

(1) The user of a safe shall be the only person who knows the lock code of the corresponding safe.

(2) A lock code shall not consist of a row of numbers or letters which can easily be guessed, such as dates of important personal days, telephone numbers, arithmetical sequences.

- (3) A lock code shall be changed:
- 1) following a change of user;
 - 2) following opening in the absence of the user;
 - 3) if there is reason to believe that the code has become known to an unauthorised person;
 - 4) twelve months after the previous change.

§ 76. Keys and locks of safes

- (1) During work-time, the user of a safe shall keep the keys of the safe.
- (2) Upon leaving the workplace, the key shall be locked away in the key cabinet.
- (3) The lock of a safe shall be changed if there is reason to believe that an unauthorised person may have gained possession of the key of the safe.

§ 77. Key cabinet

- (1) A key cabinet shall be made of metal, be lockable and be under continuous surveillance.
- (2) If a key cabinet is used by several persons, it shall be guaranteed that each user gets only the key that he or she needs.

§ 78. Storage of spare keys and lock codes

- (1) The spare keys and safe codes of a safe shall be given to the person appointed by the guidelines for protection of state secrets and the person shall keep them in a separate safe.
- (2) The spare keys and safe codes of a safe may be kept in a safe deposit box at a bank.
- (3) It is prohibited to make other notes of the codes to locks of safes.

§ 79. Keys to cabinets or drawers used for storage of media classified as restricted

The keys to a cabinet or drawer used for the storage of media classified as restricted shall be kept in a manner that prevents access thereto by unauthorised persons.

Division 5

Reproduction of and Making of Extracts from Classified Media

§ 80. Principles of reproduction

(1) Processing units shall prevent the unmonitored reproduction of and making of extracts from classified media.

(2) It is prohibited to reproduce or make extracts from media classified as top secret or secret without the written permission of the processing unit which prepared the media.

Classified information may be reproduced without specific consent for the purposes of using it in the processing system of the processing unit.

(3) Only the registrar may reproduce and make excerpts of media classified as secret or top secret.

(4) Information recorded in the means of reproduction in the course of reproduction shall be protected against unlawful access.

§ 81. Reproduction equipment

(1) Reproduction equipment used for the reproduction of media classified as confidential, secret or top secret shall be situated in a security area and the processing unit shall ensure that unauthorised persons do not have access to such reproduction equipment. Only reproduction equipment prescribed for the reproduction of and making excerpts from classified media shall be used for the reproduction of and making excerpts from classified media.

(2) Reproduction of and making excerpts from media classified as restricted is permitted only by using reproduction equipment used for such purposes which is situated in a security area.

Division 6

Destruction of Classified Media

§ 82. Principles for destruction of classified media

(1) Equipment for the destruction of media classified as confidential or at a higher level of classification shall be located within a security area.

(2) Classified media which has become unusable shall be destroyed at the earliest possible opportunity unless it is necessary to preserve it for a specific purpose.

§ 83. Destruction of classified media

(1) A paper shredder used for the destruction of paper media classified as confidential or at a higher level of classification shall shred the paper into pieces not larger than 2 x 15 mm.

- (2) A paper shredder used for the destruction of paper media classified as restricted or shall shred the paper into pieces not larger than 4 x 40 mm.
- (3) The equipment to be used for the destruction of removable storage media shall be approved by the Information Board.
- (4) Equipment not specified in subsections (1)-(3) may be used for the destruction of classified data media with the consent of the Security Police Board, the Headquarters of the Defence Forces or the Information Board, correspondingly.

§ 84. Destruction of classified media by legal persons

- (1) Legal persons in private law possessing classified information shall forward, for destruction, the media classified as confidential or at a higher level of classification, including originals, copies and extracts, to the agency which prepared the classified media or the authority which supported the application for the access permit by the legal person.
- (2) A legal person may also independently destroy the classified media specified in subsection (1) in conformity to the requirements established by this Regulation.

§ 85. Natural persons destroying classified media

- (1) At least two persons shall participate in the destruction of media classified as confidential or at a higher level of classification who shall sign the statement concerning the destruction of the classified media.
- (2) The persons who participate in the destruction shall have the right to access state secrets of the corresponding classification.

§ 86. Statement for destruction of classified media

- (1) Upon destruction of a classified medium, a statement concerning the destruction of the classified medium shall be compiled.
- (2) The following shall be included in the statement concerning the destruction of a classified medium:
 - 1) data which identifies the classified medium;
 - 2) the data of the persons who destroyed the medium;
 - 3) the method of destruction.
- (3) Statements concerning the destruction of classified media shall be preserved in the security area for at least five years.

(4) Unregistered copies of media classified as confidential or at a lower level of classification may be destroyed without preparing a statement concerning the destruction of classified media.

Division 7

Forwarding of Classified Media

Subdivision 1

General Principles of Forwarding Classified Media

§ 87. Right of recipient to access classified information of relevant level of classification

A possessor of a state secret shall ascertain before forwarding the classified medium that the recipient of the classified medium has the right to access classified information of relevant level of classification.

§ 88. Packaging for forwarding classified media General

- (1) For forwarding a classified medium, such medium shall be contained in non-transparent packaging.
- (2) The classified medium shall be packed in a safe manner which enables the fact of the packaging being opened to be subsequently ascertained. Where necessary, additional measures shall be taken to protect the contents of the package against access by unauthorised persons.
- (3) The outer package shall set out the name of the processing unit, the registration numbers of the media contained in the package and where necessary, an address.
- (4) The inner packaging shall set out, as the addressee, the register for classified media of the receiving processing unit, the level of classification of the medium in the package, the registration number and number of units.

§ 89. Organisation of forwarding

- (1) Upon forwarding a classified medium, the unit forwarding the medium and the unit receiving the medium shall agree on the forwarding in conformity to the requirements provided by this Regulation.

(2) If the processing unit cannot comply with the requirements established for the forwarding classified media, it shall address the Security Police Board or the Headquarters of the Defence Forces for the organisation of the forwarding of the classified medium.

§ 90. Manner of forwarding

- (1) Classified media shall be forwarded in a manner which takes account of the principle of need-to-know.
- (2) Classified media shall be forwarded without delay. Classified media shall be forwarded using the shortest possible journey and safest manner.
- (3) A courier shall keep a classified medium in his or her own direct possession at all times until the classified medium has been handed over.
- (4) If it is not possible to immediately forward a medium classified as confidential or at a higher level of classification, the medium shall be returned to the registrar or the person organising the protection of state secrets.
- (5) Media classified as restricted may also be sent by post as registered items with advice of delivery. The delivery notice shall be stored at the register.

§ 91. Right of courier to access classified information

A courier shall have the right to access information of the relevant level of classification in order to forward media classified as confidential or at a higher level of classification.

§ 92. Taking classified media out of security area

Media classified as confidential or at a higher level of classification may be taken out of a security area only at the permission of the head of the processing unit, registrar or other person appointed by the guidelines for the protection of state secrets of a processing unit in a lockable bag or box intended for transportation or in a sealed bag for diplomatic mail.

§ 93. Statement of delivery and receipt of classified media

- (1) The person forwarding a classified medium shall prepare a statement of delivery and receipt concerning the forwarding. Such statement need not be prepared concerning the forwarding of a medium classified as restricted.
- (2) The following shall set be out in a statement of delivery and receipt:
 - 1) the date of preparation of the medium, registration number, highest level of classification and number of forwarded units. The title of the classified medium contained in

the packaging shall not be indicated in the statement of delivery and receipt, nor shall any other reference to the content of the medium be made;

- 2) the name and address of the processing unit who is the addressee;
 - 3) the name and signature of the recipient;
 - 4) the name and signature of the deliverer.
- (3) The recipient shall sign the statement of delivery and receipt after comparing the entries on the forwarded package and in the statement.
- (4) Instrument of delivery and receipt shall be preserved with the register in a security area for at least five years.
- (5) One and the same statement of delivery and receipt may set forth the forwarding of several classified media.

§ 94. Obligations of recipient of classified media

- (1) Upon receipt of a classified medium it shall be verified whether the consignment is whole, unopened and without traces of tampering.
- (2) The registrar or other person provided in the guidelines for the protection of state secrets shall be immediately informed if a consignment has been opened, there are traces of tampering or there is any doubt in this respect.
- (3) After opening the outer packaging, the inner package shall be forwarded for registration to the registrar who shall send it forward pursuant to the procedure provided by the guidelines for the protection of state secrets.
- (4) The registrar shall verify whether the media and the contents thereof correspond to the number of units set out.

Subdivision 2

Forwarding of Classified Media from One Security Area to Another through Administrative Area

§ 95. Persons forwarding classified media through administrative area

- (1) A person may forward media classified as confidential or at a lower level of classification through an administrative area in person or through a registrar or courier.
- (2) Only a registrar, who may use a courier, is permitted to forward media classified as state secret or at a higher level of classification through an administrative area.

§ 96. Preclusion of general requirements for forwarding classified media through administrative area

§§ 88 and 92 do not apply to forwarding of classified media from one security area to another.

Subdivision 3

Forwarding of Classified Media through Public Space

§ 97. Forwarding of classified media by two natural persons

Media classified as secret or at a higher level of classification shall be forwarded by two persons. With the permission of the Security Police Board, the General Staff of the Defence Forces, the authorised representative of national security and the Information Board, such media may be forwarded by one person.

§ 98. Use of vehicles in forwarding classified media through public space

- (1) As a general rule, media classified as secret or at a higher level of classification shall be forwarded using a motor vehicle.
- (2) The windows of the vehicle shall be kept shut and the doors locked and the driver must be in an employment or service relationship with the processing unit.
- (3) The persons specified in § 99 shall not drive a vehicle while forwarding the medium.

§ 99. Carrying weapons upon forwarding classified media through public space

A courier forwarding media classified as top secret shall carry a military or service weapon or a person carrying a military or service weapon shall accompany the courier.

Subdivision 4

Forwarding of Classified Media to, in and from Foreign Countries

§ 100. Forwarding of classified media to, in and from foreign countries by courier

- (1) Media classified as confidential or at a higher level of classification shall be forwarded to, in and from foreign countries by diplomatic or military courier who has access to classified information of the relevant level.
- (2) The Security Police Board, the General Staff of the Defence Forces, the authorised representative of national security or the Information Board correspondingly may give written permission for forwarding the media specified in subsection (1) without a diplomatic or

military courier if using a diplomatic or military courier would result in undesirable delay or if the need to use a different manner of forwarding is dictated by the concrete situation.

(3) The permission specified in subsection (2) shall include the requirements which must be observed upon forwarding the consignment, above all concerning the journey and the means of transport to be used for forwarding the consignment.

§ 101. Courier for forwarding classified information to, in and from foreign countries

(1) A courier who forwards classified information to, in and from foreign countries must have a certificate of diplomatic courier issued by the Ministry of Foreign Affairs, or diplomatic immunity.

(2) For forwarding classified media in areas of military missions, a courier shall have the certificate of a military courier issued by the Ministry of Defence.

Division 8

Communication of Classified Information via Technical Communication Channels

§ 102. Use of accredited systems

Communication of classified information via technical communication channels is permitted only by using systems accredited for communication of classified information of the relevant level.

§ 103. Communication of classified information via technical communication channels in emergencies

(1) Classified information, except for information classified as top secret may be transmitted by means of a system not accredited, on the requisite level, for the transmission of classified information only in emergencies and based on the single permit granted by the head of the unit in possession of the classified information. The head of the state agency which possesses the classified information may grant permission if the rapid transmission of the classified information is unavoidable and crypting of the state secret is impossible due to lack of time or absence of the corresponding means. The Security Police Board and the Information Board shall be notified of the unencrypted transmission of classified information at the earliest opportunity.

(2) If an unaccredited system is used for transmission of classified information of foreign states, the authorised representative of national security shall be immediately informed

thereof, except in the case specified in subsection 52 (3) of the State Secrets and Classified Information of Foreign States Act.

Division 9

Information Security

§ 104. Definitions

In this Division, the following definitions are used:

- 1) "information security or InfoSec" means the ensuring of the availability, confidentiality and integrity of information in the systems processing classified information;
- 2) "accreditation of processing systems" means the assessment of the conformity of processing systems to InfoSec requirements;
- 3) "availability" means the possibility to use and access information at the request of authorised persons;
- 4) "confidentiality" means the unavailability or incomprehensibility of information to unauthorised persons;
- 5) "integrity" means the fact of it being impossible for information to be altered or deleted by unauthorised persons;
- 6) "threat" means the potential damaging of the availability, confidentiality and integrity of information;
- 7) "breach of security" means a situation where information or system operations and devices which support the protection of information have lost or could have lost their confidentiality, integrity or availability (including loss of information, communication of information to unauthorised persons, amendment or destruction of information by unauthorised persons or attack against the system) due to theft, sabotage, acts of terrorism, other prohibited activities or vulnerabilities;
- 8) "security risk" means the probability of occurrence of breaches of security;
- 9) "risk management" means the assessment of assets, information, threats, breaches of security and security risk on the basis of which the security measures for information or system operations and devices which support the protection of information are determined. Risk management includes the planning, organisation, use and monitoring of the security measures of a system in order to prevent security risks exceeding from the acceptable boundaries, and breaches of security;

- 10) “vulnerability assessment” means the detailed monitoring of the system in order to identify the vulnerabilities of the system, threats to the confidentiality, integrity and availability of information processed in the system and the vulnerability of the system to any attack or threat;
- 11) "System Specific Security Requirement Statement" means a list of security requirements mandatory for the system which provides how to achieve sufficient security of the system and how to monitor the security of information in the system;
- 12) “Security Operation Procedures” means a document which provides a detailed description of the procedure for compliance with the security requirements prescribed in the System Specific Security Requirement Statement and the duties of each specific employee or other person upon ensuring the security of information;
- 13) "Global Security Environment" means the environment surrounding the location of the system, including the building or area, in which the occurring of changes could influence the safety of the system;
- 14) "Local Security Environment" means the premises or space bordering on the Global Security Environment where the components of a system are located or used;
- 15) "Electronic Security Environment" is restricted to the components of the system which are used for the electronic processing of information and in protection of which the personnel operating the system applied electronic security measures.

§ 105. InfoSec principles

- (1) This Division provides for InfoSec principles for the protection of classified information upon the electronic processing thereof.
- (2) Classified information shall be electronically processed in processing systems prescribed for classified information which conform to InfoSec requirements and which have a conformity certificate or temporary permit for use issued by the Information Board.
- (3) Classified information shall be processed only by means of computers and local area networks situated within a Local Security Environment.
- (4) A computer used for processing information classified not higher than at the restricted level may be taken out of a Local Security Environment if:
 - 1) the classified information has been crypted by conforming means of crypting;
 - 2) the computer bears no marking which would refer to the level of classification of the information processed therein.

(5) Upon ensuring information security in protection of classified information of foreign states, the requirements prescribed by the originator of the classified information of foreign states shall also be taken into account.

(6) Ensuring information security shall, above all, adhere to the following security principles:

- 1) only the functions, protocols or services which are necessary for the processing of information or ensuring its security shall be used - the principle of minimality;
- 2) managing security risks of the system, including prevention, reduction, diversion and permitted accepting of such risks - the principle of continuous security risk management - and regular checking of system security shall be carried out on an ongoing basis;
- 3) the users and administrators of the system shall have only user privileges needed for the performance of their tasks - the principle of least privilege;
- 4) all other systems connected to the system shall be presumed to be unreliable and sufficient security measures shall be applied when exchanging information with them - the principle of self-protecting nodes;
- 5) if one of the used security measures fails, the entire system must not lose its security - the principle of defence-in-depth.

§ 106. Requirements for processing systems

(1) Systems for processing classified information shall ensure the availability, confidentiality and integrity of information.

(2) A classified information processing system shall allow:

- 1) identification and registration of persons who had or may have had access to classified information and system operations and devices which support the protection of state secrets;
- 2) identification of the users of the system based on their rights to access classified information;
- 3) access to information and system operations and devices which support the protection of information only upon existence of the right of access and a justified need to know;
- 4) verification of the confidentiality, integrity, availability and the origin, reliability and connections of information or system operations and devices which support the protection of information;
- 5) achievement of a situation where the InfoSec security mechanisms function in compliance with the requirements during the whole period of use of the system;

- 6) prevention and elimination of breaches of security and prevention and reduction of damage caused thereby;
 - 7) handling of breaches of security in the course of which threats to the system or parts thereof, damage caused thereby to information and measures taken for the elimination of the damage are determined and registered.
- (3) Information concerning a system shall be documented in the System Specific Security Requirement Statement and the Security Operation Procedures.
 - (4) Processing units perform continuous risk management of the systems.

§ 107. System Specific Security Requirement Statement

- (1) System Specific Security Requirement Statements shall set out:
 - 1) the technical specification of the system;
 - 2) an overview of the results of the assessment of the risk of a system;
 - 3) a description of the security requirements for the system;
 - 4) list of security measures applied in the system;
 - 5) description of organisation of system security.
- (2) The System Specific Security Requirement Statements shall be prepared by processing units. Before construction or commencement of use of a new system intended for the processing of classified information, the processing unit shall obtain the approval of the Information Board for the Statement.
- (3) The System Specific Security Requirement Statement shall be specified in the course of building and use of the system if changes occur, for example, the purpose or structure of the system changes, new significant threats appear or the level of classification of the information processed in the system changes. The processing unit shall obtain the approval of the Information Board for the amendments to the System Specific Security Requirement Statement.

§ 108. Security Operation Procedures

- (1) The Security Operation Procedures shall set out:
 - 1) the tasks, rights and obligations of the persons responsible for the security of the system;
 - 2) the users of the systems and their tasks, rights and obligations;
 - 3) a description of the configuration administration of the hardware and software of the system;

- 4) guidelines for the electronic processing of classified information;
 - 5) a description of the processing of the data media used within the system;
 - 6) a description of the review of the log files and incident administration.
- (2) A processing unit shall prepare the Security Operation Procedures based on the System Specific Security Requirement Statement and coordinate them with the Information Board before the processing of classified information is commenced in the system.
- (3) The Security Operation Procedures shall be specified in the course of use of the system if changes occur, for example, the purpose or structure of the system changes, new significant threats appear or the level of classification of the information processed in the system changes. All amendments to the Security Operation Procedures shall be approved by the Information Board.

§ 109. Accreditation of system

- (1) The purpose of accreditation of a system is to demonstrate that the system complies with the requirements established for ensuring information security.
- (2) The Information Board shall base the accreditation of a system on the following:
 - 1) the physical security measures of the system;
 - 2) security risks related to the system;
 - 3) the System Specific Security Requirement Statement;
 - 4) the Security Operation Procedures;
 - 5) results of radiation security zoning of the location of the system;
 - 6) information on the conformity of the InfoSec requirements by the processing unit.
- (3) The Information Board shall initiate the accreditation of a system at the initiative of the processing unit or at its own initiative. The processing unit shall annex the System Specific Security Requirement Statement and Security Operation Procedures to the application for accreditation of the system. The processing unit shall submit the rest of the information specified in subsection (2) at the request of the Information Board.
- (4) As a result of accreditation, the processing unit is issued a certificate of conformity by a directive of the director general of the Information Board.
- (5) As a result of accreditation, a temporary permit for use is issued to a system by a directive of the director general of the Information Board.
- (6) If a system does not conform to the InfoSec requirements, the Information Board shall refuse to issue a certificate of conformity or temporary permit for use to a system or shall

prohibit its use for processing classified information. A corresponding decision is made by a directive of the director general of the Information Board.

§ 110. Obligation to provide information

A processing unit is required to immediately provide information, including in written form, at the request of the Information Board concerning the system in its possession and the circumstances relating to information security, and to ensure the Information Board with access to the parts of the system regardless of their location which, during office hours, must be granted on a continuous basis and during rest days and national holidays shall be agreed upon in advance.

§ 111. Procedure for extension of certificate of conformity and temporary permit for use

- (1) A processing unit wishing to extend a certificate of conformity shall submit the Information Board a corresponding application at least two months prior to the expiry of the certificate of conformity.
- (2) The Information Board may extend the term of a temporary permit for use at its own initiative or based on a corresponding application of the processing unit.
- (3) The provisions concerning accreditation apply to the extension of certificates of conformity and temporary permits for use.

§ 112. Revocation of certificates of conformity and temporary permits for use

- (1) The Information Board shall revoke a certificate of conformity or temporary permit for use:
 - 1) based on an application by the processing unit;
 - 2) if the processing unit has failed to comply with a precept issued by the Information Board for elimination of a violation of an InfoSec requirement or a danger of such violation;
 - 3) if circumstances which are the basis for refusal to issue a certificate of conformity or temporary permit for use become evident.
- (2) A certificate of conformity or temporary permit for use shall be revoked by a directive of the director general of the Information Board.
- (3) A processing unit shall be notified of the revocation of the certificate of conformity or temporary permit for use in writing.

§ 113. Notification of authorised representative of national security

If a classified information of foreign states is processed in a system, the Information Board shall notify the authorised representative of national security of the issue of a certificate of conformity or temporary permit for use, and of the extension or revocation of a certificate of conformity.

Division 10

Protection of Classified Information of Foreign States

Subdivision 1

Processing of Classified Information of Foreign States

§ 114. Principles of processing of classified information of foreign states

Classified information of foreign states shall be processed on the same bases and pursuant to the same procedure as the processing of state secrets, taking account of the difference arising from international agreements. The requirements for processing provided in this Division do not apply to cryptomaterials registered by the Information Board and the information specified in subsection 52 (3) of the State Secrets and Classified Information of Foreign States Act.

§ 115. Keeping records of media containing classified information of foreign states

Record of media containing classified information of foreign states shall be kept separately from the records concerning state secrets such that restriction of access to register data and data media based on the need to know and right of access can be guaranteed. Separate record shall be kept in the register concerning each originator of classified information of foreign states.

§ 116. General register of classified information of foreign states maintained by authorised representative of national security

The authorised representative of national security shall keep the general register of classified information of foreign states which registers all the data media containing information of foreign states classified as secret or at a higher level of classification which have been forwarded to the state or have been created in the state, and collects data concerning media containing information of foreign states classified as confidential which have been forwarded to the state or have been created in the state.

§ 117. Register of classified information of foreign states maintained by processing units

(1) A unit processing classified information of foreign states shall establish a register of classified information of foreign states and inform the authorised representative of national security thereof beforehand in writing.

(2) A processing unit wishing to process information of foreign states classified as top secret or bearing a special marking such as ATOMAL; BOHEMIAN or other similar marking, and to maintain a corresponding register and its sub-registers shall obtain written permission to such effect from the authorised representative of national security. The authorised representative of national security shall grant the permission after conducting an inspection in the course of which it shall be established whether the requirements for processing have been met.

§ 118. Registration of media containing classified information of foreign states

(1) In addition to the register kept by a processing unit, the processing unit in possession of classified information of foreign states is required to register media containing information of foreign states classified as secret or at a higher level of classification or bearing special markings in its possession in the general register maintained by the authorised representative of national security at the first opportunity but not later than seven days after the creation of a classified medium or arrival of such medium at the processing unit.

(2) A processing unit in possession of media containing information of foreign states classified as confidential shall forward information concerning such data media to the authorised representative of national security within one month after the creation of a classified medium or arrival of such medium at the processing unit.

(3) The media forwarded to a processing unit by the authorised representative of national security need not be registered by the processing unit in the general register maintained by the authorised representative of national security.

(4) A processing unit in possession of classified information of foreign states is required to enter the registration number issued by the authorised representative of national security on every data medium which contains information of foreign states classified as secret or at a higher level of classification or bearing special markings.

§ 119. Forwarding of media containing classified information of foreign states

(1) Media containing information of foreign states classified as top secret or bearing special markings shall be received and forwarded to other processing units only through the authorised representative of national security except in cases where the authorised representative of national security has issued written consent for forwarding to the processing unit maintaining a register.

(2) The authorised representative of national security shall be informed of the forwarding of media containing information of foreign states classified as secret or at a lower level of classification within one month after the forwarding of such media.

(3) Media containing classified information of foreign states shall be forwarded only to processing units who have established a register for classified information of foreign states beforehand.

§ 120. Reproduction and destruction of media containing information of foreign states classified as top secret or bearing special markings

(1) Media containing information of foreign states classified as top secret or bearing special markings shall be reproduced and destroyed only by the authorised representative of national security.

(2) The authorised representative of national security may give a state agency written permission for the reproduction or destruction of the data media specified in subsection (1).

§ 121. Return of media containing information of foreign states classified as top secret or bearing special markings

(1) A processing unit maintaining a register of media containing information of foreign states classified as top secret or bearing special markings of foreign states shall return the media containing such information to the authorised representative of national security immediately after the need for its use is over.

(2) If it is necessary to use the data medium longer than for one year after receipt of the medium, the keeping of the medium for such extended period shall be registered in the general register maintained by the authorised representative of national security.

§ 122. Inspection by authorised representative of national security

The authorised representative of national security shall conduct, at least on one occasion over a two year period, an inspection of the security measures applied for the protection of classified information of foreign states and the right of access of the persons processing such

information in the processing units possessing classified information of foreign states. The authorised representative of national security shall conduct such inspection in agencies in possession of information classified as secret or at a higher level of classification or bearing special markings at least on one occasion after every eighteen months.

Subdivision 2

Procedure for Issue, Refusal to Issue, Extension and Revocation of Certificates for Access to Classified Information of Foreign States, and Grant, Refusal to Grant and Extension of Right of Access to Classified Information of Foreign States

§ 123. Access to classified information of foreign states

- (1) A certificate for access to classified information of foreign states (hereinafter access certificate) shall be issued for accessing classified information of foreign states if an international agreement prescribes the issue of a certificate for access to classified information of foreign states of the corresponding level of classification.
- (2) In cases prescribed by international agreements, the authorised representative of national security shall also issue a confirmation of right of access to classified information of foreign states (hereinafter confirmation).
- (3) The right for persons specified in subsections 27 (1) and (2) of the State Secrets and Classified Information of Foreign States Act to access information of the European Union and the North Atlantic Treaty Organisation classified as restricted arises after the persons have been communicated the information specified in § 130, signed the obligation and the notice specified in § 131 has been issued.
- (4) The right for natural persons and legal persons in private law to access or process classified information of foreign states arises only based on an access certificate.

§ 124. Access certificate must correspond to level of access permit to state secrets

An access certificate shall not be issued at a higher level of classification than the level of the permit to access or process state secrets held by the natural person or processing unit for whom the access certificate is applied.

§ 125. Term of access certificates

- (1) The authorised representative of national security shall decide on the term of an access certificate based on the desired term of validity indicated in the application, the term of the

right to access state secrets and the justification of the need to know. An access certificate shall not have a longer term than the right of the person to access state secrets.

(2) If a person's right to access state secrets expires before the end of the term of validity specified in the access certificate, the access certificate shall expire.

(3) If an access certificate becomes invalid on an earlier date than the date of expiry set forth in the certificate, the access certificate shall be returned to the authorised representative of national security.

§ 126. Application for access certificates for natural persons

A processing unit wishing to apply for an access certificate for a natural person shall submit the following documents to the authorised representative of national security:

1) a written application which shall set out the originator of the classified information of the foreign state, the level of classification of information for which access is applied, the requested term of validity of the access certificate, and the name and personal identification code or, in the absence thereof, date of birth of the person, exact birthplace, citizenship and contact details;

2) a copy of the access permit or other document in proof of the right to access state secrets;

3) a copy of both sides of the identity document of the person or from the page of the passport which contains personal data.

§ 127. Application for right to access to information of foreign states classified as restricted

(1) An agency or constitutional institution wishing to apply for the right to access to information of foreign states classified as restricted for a person specified in subsection 123

(3) shall submit a written application to the authorised representative of national security which shall set out the name, personal identification code and position of the person and to which a copy of the document shall be annexed by which the person is granted access to state secrets classified as restricted.

(2) Where necessary, the authorised representative of national security shall also issue confirmation in proof of the person's right to access information of foreign states classified as restricted.

§ 128. Application for access certificates for persons processing classified information based on processing permit

In order to apply for an access certificate for a person processing classified information based on a processing permit, the agency applying for grant of access shall submit the following documents to the authorised representative of national security:

- 1) a written application by the processing unit which sets out the level of classification of information for which access is applied and justifies the need of the person to access classified information of foreign states;
- 2) a written application by the supporting authority which specifies the originator of the classified information of foreign states and the level of classification for which access is applied and shall justifies the need of the person to access classified information of foreign states, unless the supporting authority is the authorised representative of national security;
- 3) a copy of the processing permit;
- 4) a copy of the guidelines for protection of state secrets;
- 5) a copy of the document for appointment of the person organising the protection of state secrets in the legal person, his or her name, and a list of persons who will process classified information of foreign states and, where necessary, the documents needed for application of access certificates for natural persons to such persons.

§ 129. Deciding on grant of access certificates based on applications

- (1) If an application for an access certificate or the documents appended thereto do not confirm to requirements, the authorised representative of national security shall inform the processing unit who applied for an access certificate for a natural person or the agency which applied for an access certificate for a processing unit of the deficiencies within ten working days and give them a term for elimination thereof.
- (2) The authorised representative of national security shall decide on the grant of or refusal to grant an access certificate within one month after the receipt of the conforming application. The term may be extended with good reason by notifying the applying or supporting agency or constitutional institution thereof.

§ 130. Communication of requirements for protection of classified information of foreign states

- (1) Before a natural person is granted the right to access information of foreign states classified as restricted or issued an access certificate for the first time, the authorised representative of national security or an agency authorised thereby shall communicate the bases for protection of classified information of foreign states to the person. Where

necessary, the authorised representative of national security shall also communicate such information to a person in the case of repeated grant of an access certificate or right of access, or issue of a confirmation.

(2) If the right to access information of foreign states classified as restricted or an access certificate is granted to a processing unit, the person organising the protection of state secrets in such unit is communicated the bases for protection of state secrets.

(3) Before handing over an access certificate or notice, the authorised representative of national security shall obtain the signature of the natural person receiving the right of access or access certificate concerning his or her obligation to maintain the confidentiality of the classified information of foreign states which becomes known to him or her by virtue of employment or service.

§ 131. Forwarding of access certificates and notices

The authorised representative of national security shall forward an access certificate or notice within five days after the creation of the right to access information of foreign states classified as restricted to the processing unit who applied for access to the agency who supported the access of a legal person. The processing unit whose application for access was supported shall be forwarded a copy of the access certificate.

§ 132. Preparation of access certificates

(1) An access certificate is prepared on letter-head with security features of the authorised representative of national security and confirmed with the signature of the head of the authorised representative of national security. An access certificate shall set out at least the following information:

- 1) date of issue and number;
- 2) the given name, surname, date of birth and place of birth of the natural person who obtains the access certificate or the name, address and registry code of the legal person who obtains the access certificate;
- 3) the highest level of classification of information of foreign states and special categories of information which the person is permitted to access;
- 4) term of validity of access certificate;
- 5) the name, time and place of the event for participation in which access was applied, as necessary.

(2) An access certificate shall be prepared in Estonian and English.

§ 133. Application and formalisation of confirmation

- (1) A processing unit wishing to receive confirmation shall submit an application to this effect and append documents thereto concerning the event for participation in which the confirmation is requested and, at the demand of the authorised representative of national security, also additional documents if this arises from a foreign agreement.
- (2) The requirements for preparation of access certificates shall be adhered to upon formalisation of a confirmation.

§ 134. Revocation of access certificates

An access certificate shall be revoked if:

- 1) the person's need to know expires;
- 2) a new access certificate is issued before the previous access certificate expires;
- 3) personal information entered in the access certificate change;
- 4) a fact precluding the issue of the access certificate become known during the time of validity of the issued access certificate.

§ 135. Notification of expiry of access permit, processing permit, right of access or need to access

The processing unit who applied for the grant of the right of access to classified information of foreign states to a natural person or an agency or constitutional institution who supported the application of a processing unit shall immediately inform the authorised representative of national security of the expiry of the need to access classified information of foreign states, or the expiry of the permit for access to state secrets or the permit for processing state secret of the person who was granted the right of access.

§ 136. Notification of authority competent to carry out security checks

The authorised representative of national security shall immediately inform the authority competent to carry out security checks with respect to a person of the grant of the right to access classified information of foreign states or issue of an access certificate to a natural or legal person, and of the revocation or establishment of the nullity of such right.

Establishment of Forms for Consent, Confirmation, Applications for Access Permit, Processing Permit and Application for Extension thereof, and Forms Completed by Applicants for Access Permit and Processing Permit and Applicants for Extension thereof

§ 137. Forms related to permits for accessing state secrets

- (1) A natural person shall submit an application for a permit to access state secrets (hereinafter access permit) using the form specified in Annex 1.
- (2) A natural person shall submit an application for the extension of an access permit using the form specified in Annex 2.
- (3) Upon application for an access permit, a natural person shall fill out the form completed by applicants for access permit (Annex 3).
- (4) Upon application for the extension of an access permit, a natural person shall fill out the form completed by applicants for extension of access permit (Annex 4).
- (5) Upon application for an access permit or extension of an access permit, a natural person shall fill out the consent form (Annex 5) annexed to the application form.
- (6) Upon application for an access permit or extension thereof, a natural person shall confirm that he or she is aware of the requirements for the protection of state secrets, the liability for violation of such requirements and the obligation to maintain the state secrets made known to him or her (Annex 6).

§ 138. Forms related to permits for processing state secrets

- (1) A legal person shall submit an application for a permit to process state secrets (hereinafter processing permit) using the form specified in Annex 7.
- (2) A legal person shall submit an application for the extension of a processing permit using the standard format specified in Annex 8.
- (3) Upon application for a processing permit, a legal person shall fill out the standard format completed by applicants for processing permit (Annex 9).
- (4) Upon application for the extension of a processing permit, a legal person shall fill out the standard format completed by applicants for extension of processing permit (Annex 10).
- (5) Upon application for a processing permit or extension of a processing permit, a legal person shall fill out the consent form (Annex 11) annexed to the application form.
- (6) Upon application for a processing permit or extension thereof, a legal person shall confirm awareness of the requirements for the protection of state secrets, liability for violation

of such requirements and obligation to maintain the state secrets made known thereto (Annex 12).

(7) Subsections (1)-(6) also apply to self-employed persons.

Chapter 7

Implementation of Regulation

§ 139. Entry into force of Regulation

- (1) This Regulation enters into force on 1 January 2008.
- (2) Clauses 8 (1) 4), 5), 7), 8) and 11) enter into force on 1 January 2009, except with respect to information which was a state secret before 1 January 2008.
- (3) Subsection 70 (1) enters into force on 1 January 2009.

Annex 1 to Government of the Republic Regulation No. 262 of 20 December 2007

"Procedure for Protection of State Secrets and Classified Information of Foreign States"

_____ (authority conducting security checks) (day, month, year)

Application for permit for access to state secrets

Applicant:

(given name and surname)

Personal identification code:

Position:

(if your current position does not require an access permit, please state the position in relation to which the access permit is sought)

Please issue an access permit to state secrets classified as _____ to me.

I hereby confirm that the information presented here is accurate. I am aware that concealment of information, submission of incorrect or falsified information on my part may result in refusal to issue an access permit to state secrets or revocation of a permit.

(Signature of applicant)

Annexes:

- 1) form completed by applicant for permit for access to state secrets on _____ pages and continuation sheets _____ on pages in one original copy;
- 2) written consent of the applicant for permit for access to state secrets on 1 page, in one original copy.

Rein Lang
Minister of Justice

Annex 2 to Government of the Republic Regulation No. 262 of 20 December 2007
"Procedure for Protection of State Secrets and Classified Information of Foreign States"

(authority conducting security checks) (day, month, year)

Application for extension of permit for access to state secrets

Applicant:

(given name and surname)

Personal identification code:

Position:

Please extend the access permit to state secrets classified as _____
issued to me.

I hereby confirm that the information presented here is accurate. I am aware that concealment of information, submission of incorrect or falsified information on my part may result in refusal to issue an access permit to state secrets or revocation of a permit.

(Signature of applicant)

Annexes:

- 1) Annex to form completed by applicant for permit for access to state secrets on _____ pages and continuation sheets _____ on pages in one original copy;
- 2) written consent of the applicant for extension of permit for access to state secrets on 1 page, in one original copy.

Rein Lang

Minister of Justice

Annex 3 to Government of the Republic Regulation No. 262 of 20 December 2007

"Procedure for Protection of State Secrets and Classified Information of Foreign States"

Photo of applicant

Form completed by person applying for access to state secret classified as top secret, secret or confidential

Please respond to all the questions and if the response is negative, please state so. If any of the answers cannot be supplied in the field provided in the form, please use an additional blank sheet of paper as a continuation sheet.

I. Personal data

1. Name:

(given name(s) and surname(s))

2. Date of birth:

(day, month, year)

3. Place of birth:

(state, county, rural municipality, city)

4. Personal identification code

5. Previous names

1) _____

(name; period during which the name was used - month, year; cause of name change)

2) _____

(name; period during which the name was used - month, year; cause of name change)

3) _____

(name; period during which the name was used - month, year; cause of name change)

6. Telephone numbers

Indicate all telephone numbers used by you.

Work: _____ Home: _____

(with area code) (with area code)

Mobile: _____ Other: _____

(with area code)

Personal e-mail addresses used by you: _____

7. Citizenship

Mark an "x" to indicate your current citizenship and follow further instructions.

I am an Estonian citizen by birth Answer question a

I am an Estonian citizen but not by birth Answer questions b, c and d

I am (have been) also a citizen of another state Answer questions c and d

I am not an Estonian citizen Answer question d

a) Estonian passports and identity card

Passport:

(number, date of issue, date of expiry and issuer of passport)

Identity card:

(number, date of issue, date of expiry and issuer of identity card)

b) bases of acquisition of Estonian citizenship:

(date and basis for acquisition of citizenship)

c) Citizenship of other states

If you are or were a citizen of another state in addition to being a citizen of Estonia, what citizenship you have or had? Specify below.

(state)

d) If you are not an Estonian citizen or if are or were a citizen of another state in addition to being a citizen of Estonia, respond to the following questions

• When did you arrive in
Estonia? _____

(date)

• When do you intend to leave Estonia?

(date)

- What is the purpose of your stay in Estonia?

-
- What citizenship do you have?

-
- Please specify your passport data

(number, date of issue, date of expiry and issuer of passport)

8. Residences

List your residences during the last 7 years in order, starting with your current residence

1) /_____ up to _____/ _____

(month, year) (month, year) (city/county, street, house, apartment, postal code)

2) /_____ up to _____/ _____

(month, year) (month, year) (city/county, street, house, apartment, postal code)

3) /_____ up to _____/ _____

(month, year) (month, year) (city/county, street, house, apartment, postal code)

4) /_____ up to _____/ _____

(month, year) (month, year) (city/county, street, house, apartment, postal code)

5) /_____ up to _____/ _____

(month, year) (month, year) (city/county, street, house, apartment, postal code)

6) /_____ up to _____/ _____

(month, year) (month, year) (city/county, street, house, apartment, postal code)

9. Postal address

Specify your postal address if it is not the address of your actual residence.

(state, county, rural municipality, city, street, house, apartment, postal code, post-office box number)

II. Family and acquaintances

10. Marital status

Indicate your current marital status and indicate the data of your spouse/cohabitee (previous spouses, cohabitee) below:

Single

Divorced

Cohabiting

Sustainable relationship

Married

Separated

Widow/widower

a) spouse/cohabitee

• Name:

• Date and place of birth:

• Personal identification code::

• Nationality:

• Previous names:

• Date of marriage/beginning of cohabitation:

• Residence of spouse/cohabitee, if you do not live at the same address, and telephone number:

(city/county, street, house, apartment)

(telephone number)

• place of work and position of spouse/cohabitee, and telephone number:

b) previous spouse/cohabitee (previous spouses/cohabitees)

1) Name:

Date and place of birth:

Nationality:

Date of marriage and place of registration (state, city):

Reason for ending marriage/cohabitation (mark with an "x")

Divorce

Death of spouse

Other reason

Date of end of marriage and place of registration of divorce (state, city):

Current residence of previous spouse/cohabitee, and telephone number (if it is known to you):

(city/county, street, house, apartment)

2) Name:

Date and place of birth:

Nationality:

Date of marriage and registration (state, city):

Reason for ending marriage/cohabitation (mark with an "x")

Date of end of marriage and place of registration of divorce (state, city):

Current residence of previous spouse/cohabitee, and telephone number (if it is known to you):

(city/county, street, house, apartment)

11. Relatives and relatives by marriage

Your parents (also foster-parents), children (also foster-children), brothers and sisters; parents, sisters, brothers and children (if they are not your children and are not foster-children) of your spouse/cohabitee; persons under your guardianship or curatorship).

. If any of the above-named are dead, please also indicate the year of their death in the date of birth section.

Given name and	Relationship	Date of birth or	Place of birth	Residence
----------------	--------------	------------------	----------------	-----------

Job and position;

Please state other persons whom you deem necessary to point out or who may prove essential to the security check.

Name	Circumstances
------	---------------

1)

2)

3)

III. Education

13. Education beginning with primary education (including military education, education acquired abroad and unfinished education)

1) / _____ up to _____ / _____

(month, year) (month, year) (name of school)

Location of school:

Acquired education/degree/unfinished studies:

Courses studied/speciality:

2) / _____ up to _____ / _____

(month, year) (month, year) (name of school)

Location of school:

Acquired education/degree/unfinished studies:

Courses studied/speciality:

3) / _____ up to _____ / _____

(month, year) (month, year) (name of school)

Location of school:

Acquired education/degree/unfinished studies:

Courses studied/speciality:

4) / _____ up to _____ / _____
(month, year) (month, year) (name of school)

Location of school:

Acquired education/degree/unfinished studies:

Courses studied/speciality:

14. In-service training during the past 7 years if the training took place outside of the Members States of the EU and NATO

1) / _____ up to _____ / _____
(month, year) (month, year) (state, training provider, topic of training)

2) / _____ up to _____ / _____
(month, year) (month, year) (state, training provider, topic of training)

3) / _____ up to _____ / _____
(month, year) (month, year) (state, training provider, topic of training)

15. Language skills

1 - poor; 2 - fair; 3 - good; 4 - very good; 5 - proficient;
6 - mother tongue

Language heard spoken read written

IV. Professional activities

16. Previous professional activities (including in foreign states)

Indicate, in chronological order, all the places where you have worked (including contractual active service in the Defence Forces, second jobs, contracts with other employers, etc.).

Indicate the name of your immediate superior if it is known to you.

1) / _____ up to _____ / _____
(month, year) (month, year) (name of employer)

Address (state, city) and telephone number (with area code) of employer:

Address of workplace (if different from address of employer):

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

Reason for leaving work:

2) / _____ up to _____ / _____

(month, year) (month, year) (name of employer)

Address (state, city) and telephone number (with area code) of employer

Address of workplace (if different from address of employer):

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

Reason for leaving work:

3) / _____ up to _____ / _____

(month, year) (month, year) (name of employer)

Address (state, city) and telephone number (with area code) of employer

Address of workplace (if different from address of employer):

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

Reason for leaving work:

4) / _____ up to _____ / _____

(month, year) (month, year) (name of employer)

Address (state, city) and telephone number (with area code) of employer

Address of workplace (if different from address of employer):

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

Reason for leaving work:

5) / _____ up to _____ / _____

(month, year) (month, year) (name of employer)

Address (state, city) and telephone number (with area code) of employer

Address of workplace (if different from address of employer):

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

Reason for leaving work:

6) / _____ up to _____ / _____

(month, year) (month, year) (name of employer)

Address (state, city) and telephone number (with area code) of employer

Address of workplace (if different from address of employer):

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

Reason for leaving work:

17. Military service (also abroad)

Mark an "x" in the appropriate box (this questions does not pertain to contractual active service)

Yes/No

- 1) Have you served military service? Answer question a
- 2) Have you served alternative service? Answer question b
- 3) Have you participated in training/training exercises for reservists during the last five years? Answer question a

a) Name, number and location of military unit

Period of service

(month, year)

Service

Rank

Speciality

b) Place of alternative service

Period of service (month, year)

V. Contacts with foreign states

18. Contacts

Mark an "x" in the appropriate box.

Yes/No

a) Have you ever had contacts with a representative of a government, embassy or consulate of a foreign state, whether within or outside the territory of the Republic of Estonia, for any other reason than the official interests of the Republic of Estonia ? (Except for contacts concerning visa applications and crossing borders)?

b) Do you have assets, business contacts or financial interests in a foreign state?

c) Are you currently or have you ever been employed as a consultant in a government agency, company or organisation of a foreign state, or are you currently acting or have you acted in such role?

d) Have you ever had any contact with intelligence services of foreign states? (including the USSR)

If you answered "yes" to any of the above questions, provide an explanation in the following table.

Letter

Period (month/year)

State, company/agency/organisation

Explanation

19. Visits abroad

List, in chronological order, the foreign states you have visited in the last ten years.

Use the following codes to designate the purpose of the trip:

1 - placement 2 - tourism 3 - study 4 - other purpose

Period (month/year)

Code

Country

Period (month/year)

Code

Country

- 1)
- 6)
- 2)
- 7)
- 3)
- 8)
- 4)
- 9)
- 5)
- 10)

VI. Other relevant information

20. Participation in associations/organisations

Set out all associations (including companies), organisations, political parties (also in foreign states in which you are currently participating or have participated in the past, including engaging in entrepreneurship as a self-employed person.

Association, organisation, political party or other

Location

Time of joining/leaving/start of engaging in entrepreneurship

Your status

- 1)
- 2)
- 3)
- 4)
- 5)
- 6)
- 12

21. Health and lifestyle

Mark an "x" in the appropriate box

Yes No

Have you ever consulted a psychiatrist or psychologist? Answer question a

Have you ever had problems resulting from the abuse of alcohol (at work, at a public place, problems with health)? Answer question b

Have you ever tried narcotics or psychotropic substances? Answer question b

Do you currently use narcotics or psychotropic substances? Answer question b

Do you or have you ever gambled? Answer question b

a) If you answered yes, please give detail, indicating the name of the health care institution or consultation service provider

Time of treatment or consultation (month/year)

Description

b) If you answered yes, please give details

Period (month/year)

Description

22. Punishments

Mark an "x" in the appropriate box

Yes/No

1) Have you been punished under disciplinary procedure? Answer question a

2) Have you been punished under administrative or misdemeanour procedure? Answer question b

3) Have you been punished under criminal procedure? Answer question c

4) Have you been detained during criminal proceedings or have preventive measures been applied in respect of you? Answer question d

5) Have you participated in criminal proceedings as a suspect, accused or accused at trial? Answer question d

6) Have you been registered with the Juvenile Police or the committee for matters regarding minors?

Answer question d

a) The authority or other legal person who imposed the punishment

Time of imposition of punishment (month/year)

Basis

What kind of punishment was imposed?

1)

2)

3)

b) Authority which imposed the punishment

Time of imposition of punishment (month/year)

Basis

Type and term/category of punishment

1)

2)

3)

c) name of court

Time of imposition of punishment (day/month/year)

Type and term/category of punishment

Criminal offence committed

Place punishment served

d) When? (month/year) Where? Under which circumstances?

1)

2)

3)

23. Financial status

Mark an "x" in the appropriate box

Yes/No

1) Do you own immovable property, including joint property and common ownership (including buildings, parts thereof and apartments which are to be entered in the land register)? Answer question a

2) Do you own shares, units or other securities (except for units of pension funds)?

Answer question b

3) Do you have financial obligation in an amount exceeding your one months' salary? (including leases, credit cards, debts to private persons, rapid loans, etc.? Also specify if you are a co-applicant for a loan or providing surety for a loan of another person) Answer question c

4) Do you have any other sources of income in addition to the salary received from your principal job? Answer question d

5) Do you own any registered vehicles? (set out also the vehicles that you are using based on authorisation or a lease contract) Answer question c

6) Have you granted anybody a loan within the past five years in an amount exceeding your one months' salary? Answer question f

7) Do you have pending civil disputes? Answer question g

a) Description of immovable property

Address of location of immovable

Name of immovable property

cadastral code of the cadastral unit

1)

2)

3)

4)

5)

b) Name of issuer of share or unit

Type

Quantity

market value (in kroons)

1)

2)

3)

4)

5)

c) 1) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

2) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

3) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

4) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

d) Additional sources of income (describe)

1) _____

2) _____

3) _____

4) _____

e) Type of means of transport

Make

Year of production

Registration number

Name of owner

1)

2)

3)

f) 1) Name or title of recipient of loan

Amount of loan:

Term of loan:

2) Name or title of recipient of loan

Amount of loan:

Term of loan:

3) Name or title of recipient of loan

Amount of loan:

Term of loan:

G) Name of court

Content of summations and/or number of case

Counterparty (counterparties) of dispute

1)

2)

3)

24. Bank accounts (including accounts for funded pensions)

Bank (name and location)

Account number, currency

1)

2)

3)

4)

25. Weapons permit or parallel weapons permit

Authority who issued permit

Date of issue of permit

Weapon number

Make of weapon

In the case of a parallel weapons permit, the owner of the weapon

1)

2)

3)

26. Hobbies and special interests (describe)

1) _____

2) _____

3) _____

4) _____

VII. Information regarding application

27. Have you previously had applied for or had access to a state secret?

If you answered yes, please give details.

Period of having access

(month/year)

To what level of classification of state secrets you had access?

For what reason did you need an access permit/right of access?

1)

2)

3)

28. In addition to the permit to access state secrets, do you also need an certificate for access to classified information of foreign states?

Yes/No

If yes, please specify the issuer of the classified information of a foreign state and the level of classified information of a foreign state to which you need a certificate for access:

VIII. Other circumstances or explanations

Other circumstances or explanations which you consider significant:

(day, month, year) (signature of applicant)

Rein Lang
Minister of Justice

Annex 4 to Government of the Republic Regulation No. 262 of 20 December 2007
"Procedure for Protection of State Secrets and Classified Information of Foreign States"

Applicant

Photograph

Form completed by person applying for extension of permit to access state secrets classified
as top secret, secret or confidential

(to be filled out upon application for extension of permit to access state secrets)

Please respond to all the questions and if the response is negative, please state so unless other
instructions for answering are set out in the question. If any of the answers cannot be supplied
in the field provided in the form, please use an additional blank sheet of paper as a
continuation sheet.

I. Personal data

1. Name:

(given name(s) and surname(s))

2. Date of birth:

(day, month, year)

3. Place of birth:

(country, county, rural municipality, city)

4. Personal identification code

5. Previous names

1) _____

(name; period during which the name was used - month, year; cause of name change)

2) _____

(name; period during which the name was used - month, year; cause of name change)

6. Telephone numbers

Indicate all telephone numbers used by you.

Work: _____ Home: _____

(including the area code) (including the area code)

Mobile: _____ Other: _____

(with area code)

Personal e-mail addresses used by you: _____

7. Passport and identity card:

Passport:

(number, date of issue, date of expiry and issuer of passport)

Identity card:

(number, date of issue, date of expiry and issuer of identity card)

If your citizenship has changed during the period following your last application for a permit to access state secrets or application for extension of such permit, please submit the following data:

Bases for acquisition of citizenship:

(date and year of acquisition of citizenship)

The state whose citizenship you have acquired:

8. Residences

List your residences during the last 5 years in order, starting with your current residence

1) / _____ up to _____ / _____

(month, year) (month, year) (city/county, street, house, apartment, postal code)

2) / _____ up to _____ / _____

(month, year) (month, year) (city/county, street, house, apartment, postal code)

3) / _____ up to _____ / _____

(month, year) (month, year) (city/county, street, house, apartment, postal code)

9. Postal address

Specify your postal address if it is not the address of your actual residence.

(state, county, rural municipality, city, street, house, apartment, postal code, post-office box number)

II. Family and acquaintances

10. Marital status

Indicate your current marital status and indicate the data of your spouse/cohabitee below. If, during the period following your last application for a permit to access state secrets or application for extension of such permit, you have divorced or terminated your cohabitation with the same cohabitee, please also state the data of your previous spouse/cohabitee below:

Not married

Divorced

Cohabiting

Sustainable relationship

Married

Separated

Widow/widower

a) spouse/cohabitee

- Name:
- Date and place of birth:
- Personal identification code::
- Nationality:
- Previous names:
- Date of marriage/beginning of cohabitation:

- Residence of spouse/cohabitee, if you do not live at the same address, and telephone number:

(city/county, street, house, apartment)

(telephone number)

- place of work and position of spouse/cohabitee, and telephone number:

- b) previous spouse/cohabitee (previous spouses/cohabitees)

Name:

Date and place of birth:

Nationality:

Date of marriage and registration (state, city):

Reason for ending marriage/cohabitation (mark with an "x"):

Divorce

Death of spouse

Other reason

Date of end of marriage and place of registration of divorce (state, city):

Current residence of previous spouse/cohabitee, and telephone number (if it is known to you):

(city/county, street, house, apartment)

11. Relatives and relatives by marriage (to be filled out if there have been changes to the data during the period following your last application for a permit to access state secrets or application for extension of such permit)

Your parents (also foster-parents), children (also foster-children), brothers and sisters; parents, sisters, brothers and children (if they are not your children and are not foster-children) of your spouse/cohabitee, persons under your guardianship or curatorship;

If any of the above-named are dead, please also indicate the year of their death in the date of birth section.

Given name and surname	Relationship	Date of birth and personal identification code (if it is known to you)	Place of birth	Residence (city/county, street, house, apartment)
------------------------	--------------	--	----------------	---

Workplace (agency, location)	Position
------------------------------	----------

12. Close acquaintances and other persons whom the applicant deems necessary to point out

Indicate two persons who know you well and who are currently residing in the Republic of Estonia. The given persons shall have known you for the last 5 years. Please do not indicate your spouse/cohabitee, previous spouses/cohabitees or relatives.

1) Name and date of birth:

How long known (from year):

Telephone number:

Home or workplace address (city/county, street, house, apartment):

Job and position;

2) Name and date of birth:

How long known (from year):

Telephone number:

Home or workplace address (city/county, street, house, apartment):

Job and position;

Please state other persons whom you deem necessary to point out or who may prove essential to the security check.

Name

Circumstances

1)

2)

III. Education

13. Education (including military education, education acquired abroad and unfinished education). To be filled out if there have been changes to the data during the period following your last application for a permit to access state secrets or application for extension of such permit)

1) /_____ up to _____/ _____
(month, year) (month, year) (name of school)

Location of school:

Acquired education/degree/unfinished studies:

Courses studied/speciality:

2) /_____ up to _____/ _____
(month, year) (month, year) (name of school)

Location of school:

Acquired education/degree/unfinished studies:

Courses studied/speciality:

14. In-service training during the past 5 years if the training took place outside of the Members States of the EU and NATO

1) /_____ up to _____/ _____
(month, year) (month, year) (state, training provider, topic of training)

2) /_____ up to _____/ _____
(month, year) (month, year) (state, training provider, topic of training)

3) / _____ up to _____ / _____
(month, year) (month, year) (state, training provider, topic of training)

IV. Professional activities

15. Professional activities (including in foreign states)

Indicate, in chronological order, all the places where you have worked (including contractual active service in the Defence Forces, second jobs, contracts with other employers, etc.) after following your last application for a permit to access state secrets or application for extension of such permit.

1) / _____ up to _____ / _____
(month, year) (month, year) (name of employer)

Address (state, city) and telephone number (with area code) of employer

_____ Address of workplace (if different from address of employer):

/ _____ up to _____ / _____
(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____
(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____
(month, year) (month, year) (position and name of direct superior)

Reason for leaving work:

2) / _____ up to _____ / _____
(month, year) (month, year) (name of employer)

Address (state, city) and telephone number (with area code) of employer

_____ Address of workplace (if different from address of employer):

/ _____ up to _____ / _____
(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____
(month, year) (month, year) (position and name of direct superior)

/ _____ up to _____ / _____

(month, year) (month, year) (position and name of direct superior)

Reason for leaving work:

V. Contact with foreign states

16. Contacts

Mark an “x” in the appropriate box (the answer must pertain to the period following your last application for a permit to access state secrets or application for extension of such permit).

Yes/No

a) Have you had contacts with a representative of a government, embassy or consulate of a foreign state, whether within or outside the territory of the Republic of Estonia, for any other reason than the official interests of the Republic of Estonia (with the exception of contacts concerning visa applications and crossing borders)?

b) Do you have assets, business contacts or financial interests in a foreign state?

c) Are you currently or have you ever been employed as a consultant in a government agency, company or organisation of a foreign state, or are you currently acting or have you acted in such role?

d) Have you had any contact with foreign intelligence services?

If you answered “yes” to any of the above questions, provide an explanation in the following table.

Letter

Period (month/year)

State, company/agency/organisation

Explanation

17. Visits abroad

List, in chronological order, the foreign states you have visited during the period following your last application for a permit to access state secrets or application for extension of such permit.

Use the following codes to designate the purpose of the trip:

1 - placement 2 - tourism 3 - study 4 - other purpose

Period (month/year)

Code

Country

Period (month/year)

Code

Country

- 1)
- 6)
- 2)
- 7)
- 3)
- 8)
- 4)
- 9)
- 5)
- 10)

VI. Other relevant information

18. Participation in associations/organisations

Set out all associations (including companies), organisations, political parties (also in foreign states in which you are currently participating or have participated in the past, including engaging in business as a self-employed person (to be filled out if there have been changes to the data during the period following your last application for a permit to access state secrets or application for extension of such permit).

Association, organisation, political party or other

Seat

Time of joining/leaving/start of engaging in entrepreneurship

Your status

- 1)
- 2)
- 3)
- 8
- 4)
- 5)

19. Health and lifestyle

Mark an “x” in the appropriate box (the answer must pertain to the period following your last application for a permit to access state secrets or application for extension of such permit).

Yes/No

Have you consulted a psychiatrist or psychologist? Respond to question a

Have you had problems resulting from the abuse of alcohol (at work, at a public place, problems with health?) Respond to question b

Have you tried narcotics or psychotropic substances? Respond to question b

Do you currently use narcotics or psychotropic substances? Respond to question b

Do you or have you gambled? Respond to question b

a) If you answered yes, please explain in the following table, indicating the name of the health care institution or consultation service provider

Time of treatment or consultation (month/year)

Description

b) If you answered “yes” to any of the above questions, provide an explanation in the following table.

Period (month/year)

Description

20. Punishments

Mark an “x” in the appropriate box (the answer must pertain to the period following your last application for a permit to access state secrets or application for extension of such permit).

Yes/No

1) Have you been punished under disciplinary procedure? Respond to question a

2) Have you been punished under misdemeanour procedure? Respond to question b

3) Have you been punished under criminal procedure? Respond to question c

4) Have you been detained during criminal proceedings or have preventive measures been applied in respect of you? Respond to question d

5) Have you participated in criminal proceedings as a suspect, accused or accused at trial? Respond to question d

a) The authority or other legal person who imposed the punishment

Date (month/year) of imposition of punishment

Basis

What kind of punishment was imposed?

1)

2)

3)

b) Name of body which imposed punishment

Date (month/year) of imposition of punishment

Basis

Type and term/category of punishment

1)

2)

3)

c) Name of court

Date (month/year) of imposition of punishment

Type and term/category of punishment

Criminal offence committed

Place punishment served

d) When (month/year)?

Where?

Under what circumstances?

1)

2)

3)

21. Financial status

Mark an "x" in the appropriate box (the answer must pertain to the period following your last application for a permit to access state secrets or application for extension of such permit).

Yes/No

1) Have you acquired immovable property, including joint property and common ownership (including buildings, parts thereof and apartments which are to be entered in the land register)? Answer question a

2) Have you acquired shares, units or other securities (except for units of pension funds)? Answer question b

3) Do you have financial obligation which in an amount exceeding your one months' salary? (including leases, credit cards, debts to private persons, rapid loans, etc.? Also specify if you are a co-applicant for a loan or providing surety for a loan of another person) Answer question c

4) Do you have any other sources of income in addition to the salary received from your principal job? Answer question d

5) Do you own any registered vehicles? (set out also the vehicles that you are using based on authorisation or a lease contract) Answer question c

6) Have you granted anybody a loan within the past five years in an amount exceeding your one months' salary? Answer question f

7) Do you have pending civil disputes? Answer question g

a) Description of immovable property

the address of the immovable property

Name of immovable property

cadastral code of the cadastral unit

1)

2)

3)

4)

5)

b) name of issuer of share or shares

Type

Quantity

Market value (in kroons)

1)

2)

3)

4)

5)

c) 1) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

2) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

3) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

d) d) Additional sources of income (describe)

- 1) _____
- 2) _____
- 3) _____

e) Type of means of transport

Make

Year of production

Registration number

Name of owner

- 1)
- 2)
- 3)

f) 1) Name or title of recipient of loan

Amount of loan:

Term of loan:

2) Name or title of recipient of loan

Amount of loan:

Term of loan:

3) Name or title of recipient of loan

Amount of loan:

Term of loan:

g) Name of court

Content of summations and/or number of case

Counterparty (counterparties) of dispute

1)

2)

22. Bank accounts (including accounts for funded pensions)

To be filled out if there have been changes to the data during the period following your last application for a permit to access state secrets or application for extension of such permit)

Bank (name and location)

Account number, currency

1)

2)

3)

4)

23. Weapons permit or parallel weapons permit

To be filled out if there have been changes to the data during the period following your last application for a permit to access state secrets or application for extension of such permit)

Authority who issued permit

Date of issue of permit

Weapon number

Make of weapon

In the case of a parallel weapons permit, the owner of the weapon

1)

2)

24. Hobbies and special interests (describe)

1) _____

2) _____

VII. Other circumstances or explanations

25. In addition to the permit to access state secrets, do you also need an certificate for access to classified information of foreign states?

If yes, please specify the issuer of the classified information of a foreign state and the level of classified information of a foreign state to which you need a certificate for access:

26. Other circumstances or explanations which you consider significant:

(day, month, year) (signature of applicant)

Rein Lang

Minister of Justice

Annex 5 to Government of the Republic Regulation No. 262 of 20 December 2007

"Procedure for Protection of State Secrets and Classified Information of Foreign States"

Written consent by applicant for permit to access state secrets or applicant for extension of such permit

Applicant:

(given name and surname)

Personal identification code::

Position:

I hereby give _____ (the name of the agency conducting the security check) permission to obtain information concerning my person from natural and

legal persons and the agencies and bodies thereof in order to decide on the grant or extension of the right of access, as well as during the period of validity of my right of access.

Please assist the person presenting this letter in every way. This information is needed for the performance of the lawful duties of the agency conducting the security check and is intended only for internal use.

(day, month, year) (signature)

Rein Lang
Minister of Justice

Annex 6 to Government of the Republic Regulation No. 262 of 20 December 2007
"Procedure for Protection of State Secrets and Classified Information of Foreign States"

Confirmation by natural person to maintain state secrets made known to him or her

I, _____, personal identification code::

_____,

(given name and surname)

confirm that I am aware of the requirements concerning the protection of state secrets, the liability for violation of such requirements and my obligation to maintain the state secrets which become known to me.

I have been explained that if I fail to perform the above obligation or the obligations arising from the Classified Information of Foreign States Act or legislation issued on the basis thereof or perform them in an inadequate manner, I will be held liable in the case and pursuant to the procedure provided by law.

The obligation to maintain state secrets remains in force also after the access permit is revoked or expires.

(day, month, year) (signature)

Rein Lang
Minister of Justice

Annex 7 to Government of the Republic Regulation No. 262 of 20 December 2007

"Procedure for Protection of State Secrets and Classified Information of Foreign States"

(agency conducting security check) (day, month, year)

Application for processing state secrets

Business name/name:

Commercial registry code/personal identification code

Please issue a permit for the processing of state secrets to

(name of legal person/self-employed person)

I hereby confirm that the information presented in this application is accurate. I am aware that concealment of information, submission of incorrect or falsified information on my part may result in refusal to issue a permit to process state secrets or revocation of such permit.

(signature of the head of the legal person, or the signature of the self-employed person)

(name and office of signatory)

Annexes:

- 1) form completed by applicant for permit for processing state secrets on _____ pages and continuation sheets _____ on pages in one original copy;
- 2) written consent of the applicant for permit for processing state secrets on 1 page, in one original copy.

Rein Lang

Minister of Justice

Annex 8 to Government of the Republic Regulation No. 262 of 20 December 2007

"Procedure for Protection of State Secrets and Classified Information of Foreign States"

(agency conducting security checks) (day, month, year)

Application for extension of permit for processing state secrets

Business name, name: _____

Commercial registry code/personal identification code:

Please extend the permit for processing state secrets issued to

_____ (name of legal person/self-employed person).

I hereby confirm that the information presented in this application is accurate. I am aware that concealment of information, submission of incorrect or falsified information on my part may result in refusal to extend the permit to process state secrets or revocation of such permit.

(signature of the head of the legal person, or the signature of the self-employed person)

(name and office of signatory)

Annexes:

- 3) Annex to form completed by applicant for permit for processing state secrets on _____ pages and continuation sheets _____ on pages in one original copy;
- 4) written consent of the applicant for extension of permit for processing state secrets on 1 page, in one original copy.

Rein Lang
Minister of Justice

Annex 9 to Government of the Republic Regulation No. 262 of 20 December 2007
"Procedure for Protection of State Secrets and Classified Information of Foreign States"

Form completed by applicant for permit for processing state secrets

Please respond to all the questions and if the response is negative, please state so. If any of the answers cannot be supplied in the field provided in the form, please use an additional blank sheet of paper as a continuation sheet.

I. Data of legal person

1. Business name:

2. Date of registration:

(day, month, year)

3. Commercial registry code:

4. Previous business names:

1) _____

(business name; period during which the name was used - month, year; cause of name change)

2) _____

(business name; period during which the name was used - month, year; cause of name change)

5. Seat and address

Please indicate the legal, postal and operating address if the legal person.

1) _____

(state, county, rural municipality, city, street, house, postal code, post-office box number)

2) _____

(state, county, rural municipality, city, street, house, postal code, post-office box number)

3) _____

(state, county, rural municipality, city, street, house, postal code, post-office box number)

6. Legal form and share capital of legal person

Please specify the legal form of the legal person and state the amount of the share capital of legal person in kroons.

7. Areas of activity

- Main areas of activity

- Additional areas of activity:

8. Bank accounts

Bank (name and location)

Account number, currency

1)

2)

3)

4)

5)

9. Founders

Registry code/date of birth/personal identification code

Business name/name

Residence/seat

Size of holding

1)

2)

3)

4)

5)

6)

10. Members of the directing, control and supervisory bodies (members of management board and supervisory board) during the past five years

Role

Registry code/date of birth/personal identification code

Business name/name

Residence/seat

1)

2)

3)

4)

5)

6)

7)

8)

9)

11. Head of legal person

Name:

(given name(s) and surname(s))

Date of birth or personal identification code:

Residence:

(city/county, street, house, apartment, postal code)

Telephone number:

12. Data of the person organising protection of state secrets

Name:

(given name(s) and surname(s))

Date of birth or personal identification code:

Residence:

(city/county, street, house, apartment, postal code)

Telephone number:

13. Owners

Please specify the share/unit holders during the past 5 years whose holding has been at least 5 % of the share capital

Registry code/date of birth/personal identification code

Business name/name

Residence/seat

Size of holding

1)

2)

3)

4)

5)

6)

14. Holding of legal person in other enterprises

Registry code/date of birth/personal identification code

Business name/name

Residence/seat

Size of holding

- 1)
- 2)
- 3)
- 4)
- 5)
- 6)

15. procurement holders/authorised representatives

Forenames

Surname

Personal identification code/date of birth

Residence

- 1)
- 2)
- 3)
- 9
- 4)

State the extent of the procurement, type of authorisation and duration thereof:

16. Auditors

Forenames

Surname

Personal identification code/date of birth

Number of certificate

- 1)
- 2)

17. Participation in public procurement competitions during the past 5 years

Year

Public procurement (agency, object)

Won

Yes/No

Ordering party

18. Used subcontractors during the past 5 years

Public procurement (agency, object)

Business name/name of subcontractor

Residence/seat of subcontractor

Performed work

1)

2)

3)

4)

19. Participation as subcontractor during the past 5 years

Public procurement (agency, object)

Business name/name of main contractor

Residence/seat of main contractor

Performed work

10

1)

2)

3)

4)

20. Financial information based on annual reports during the past 5 years

Year

Balance sheet total

Profit

Loss

II. Contact with foreign states

21. Contacts with official authorities of foreign states and financial interests

Mark an "x" in the appropriate box

Yes/No

a) Has the legal person directed by you ever had contacts with a representative of a government, embassy or consulate of a foreign state for any other reason than the official interests of the Republic of Estonia (with the exception of contacts concerning visa applications and crossing borders)?

b) Does the legal person directed by you have assets or financial interests in a foreign state?

c) Has the legal person directed by you ever had any contact with foreign intelligence services?

If you answered “yes” to any of the above questions, provide an explanation in the following table.

Letter

Period (month/year)

State, company/agency/organisation

Explanation

22. Contacts with foreign agencies, enterprises and organisations

Please specify the foreign agencies, enterprises and organisations with which the legal person cooperates or has cooperated during the past 5 years.

Period (month/year)

State, company/agency/organisation

Explanation

III. Other relevant information concerning legal person

23. Violations and legal disputes

Mark an “x” in the appropriate box

Yes/No

1) Has the legal person directed by you been punished under administrative or misdemeanour procedure? Respond to question a

2) Has the legal person directed by you been punished under criminal procedure?

Respond to question b

3) Does the legal person directed by you currently have or has had arrears to the Tax Board? Answer question c

4) Has the legal person directed by you violated any procurement contracts concluded for the performance of public procurement during the past 3 years? Respond to question d

5) Has the legal person directed by you any pending civil court disputes? Respond to question e

a) Authority which imposed the punishment

Date (month/year) of imposition of punishment

Basis

Type and term/category of punishment

1)

2)

3)

b) Name of court

Date (month/year) of imposition of punishment

Type and term/category of punishment

Criminal offence committed

c) Specify the arrears

Period (month/year)

Explanation

Imposed sanctions

1)

2)

3)

d) Public procurement (agency, object)

Period (month/year)

Explanation

Imposed sanctions

1)

2)

3)

4)

e) Name of court

Content of summations and/or number of case

Counterparty (counterparties) of dispute

1)

2)

3)

24. Financial obligations

Mark an "x" in the appropriate box

Yes/No

- 1) Does the legal person directed by you own immovable property, including common ownership (including buildings, parts thereof and apartments which are to be entered in the land register)? Answer question a
- 2) Has a right of security been established with regard to the property of the legal person directed by you? Answer question b
- 3) Does the legal person directed by you have financial obligations which exceed the average one month's turnover during the preceding financial year? Answer question c
- 4) Does the legal person directed by you have obligees who have exceeded the term for performance of their obligations (payment, etc) for more than three months? Answer question d

a) Description of immovable property

Address of location of immovable

Name of immovable property

cadastral code of the cadastral unit

1)

2)

3)

4)

5)

b) The time (month/year) of creation and duration of right of security

Holder of right of security (business name/name, seat)

Object of right of security

Claim secured by right of security

1)

2)

3)

4)

5)

c) 1) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

2) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

3) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

d) Nature of proprietary obligation

Business name/name of obligee

Size of financial obligation in kroons

IV. Information regarding application

25. Has the legal person applied for or held a permit for processing state secrets or a right to access state secrets?

If you answered yes, please give details.

Period (month/year) of holding a permit for processing state secrets/ a right to access state secrets

Please specify the level of classification of the state secrets for which you held a processing permit/right of access?

Please specify the reason why you needed the permit for processing state secrets/ the right to access state secrets?

- 1)
- 2)
- 3)

Yes/No

26. In addition to the processing permit, do you also need an certificate for access to classified information of foreign states?

If yes, please specify the issuer of the classified information of a foreign state and the level of classified information of a foreign state to which you need a certificate for access:

V. Other circumstances or explanations

Other circumstances or explanations which you consider significant:

(date, month, year) (signature, name and position of legal person)

Rein Lang

Minister of Justice

Annex 10 to Government of the Republic Regulation No. 262 of 20 December 2007

"Procedure for Protection of State Secrets and Classified Information of Foreign States"

Form completed by applicants for extension of processing permit (to be filled out upon application for the extension of a permit for processing state secrets)

Please respond to all the questions and if the response is negative, please state so unless other instructions for answering are set out in the question. If any of the answers cannot be supplied

in the field provided in the form, please use an additional blank sheet of paper as a continuation sheet.

I. Data concerning legal person

1. Business name:

2. Date of registration:

(day, month, year)

3. Commercial registry code:

4. Seat and address

Please indicate the legal, postal and operating address if the legal person.

4) _____

(state, county, rural municipality, city, street, house, postal code, post-office box number)

5) _____

(state, county, rural municipality, city, street, house, postal code, post-office box number)

6) _____

(state, county, rural municipality, city, street, house, postal code, post-office box number)

5. Legal form and share capital of legal person

Please specify the legal form of the legal person and state the amount of the share capital of legal person in kroons.

6. Areas of activity

Please specify any changes that took place after your last application for the issue or extension of the permit for processing state secrets.

- Main areas of activity

- Additional areas of activity:

7. Bank accounts

Bank (name and location)

Account number, currency

1)

2)

3)

4)

5)

8. Members of the directing, control and supervisory bodies (members of management board and supervisory board) at the time of application for extension of the processing permit

Role

Registry code/date of birth/personal identification code

Business name/name

Residence/seat

1)

2)

3)

4)

5)

6)

9. Head of legal person

Name:

(given name(s) and surname(s))

Date of birth or personal identification code:

Residence:

(city/county, street, house, apartment, postal code)

Telephone number:

10. Person organising the protection of state secrets

Name:

(given name(s) and surname(s))

Date of birth or personal identification code:

Residence:

(city/county, street, house, apartment, postal code)

Telephone number:

11. Owners

Please indicate the share/unit holders who have acquired a holding in the enterprise after the last application for the issue or extension of a permit for processing state secrets and whose holding is at least 5 % of the share capital.

Registry code/date of birth/personal identification code

Business name/name

Residence/seat

Size of holding

1)

2)

3)

4)

12. Holding of legal person in other enterprises

Please specify the holding that was acquired after your last application for the issue or extension of the permit for processing state secrets.

Registry code/date of birth/personal identification code

Business name/name

Residence/seat

Size of holding

1)

2)

3)

4)

19

13. Procurement holders/authorised representatives

Please specify any changes that took place in the data after your last application for the issue or extension of the permit for processing state secrets.

Forenames

Surname

Personal identification code/date of birth

Residence

1)

2)

State the extent of the procuration, type of authorisation and duration thereof:

14. Auditors

Forenames

Surname

Personal identification code/date of birth

Number of certificate

1)

2)

15. Participation in public procurement competitions after your last application for the issue or extension of the permit for processing state secrets.

Year

Public procurement (agency, object)

Won

Yes/No

Ordering party

16. Please specify the subcontractors that you have used after your last application for the issue or extension of the permit for processing state secrets.

Public procurement (agency, object)

Business name/name of subcontractor

Residence/seat of subcontractor

Performed work

1)

2)

3)

4)

17. Please specify if you have operated as a subcontractor after your last application for the issue or extension of the permit for processing state secrets

Public procurement (agency, object)

Business name/name of main contractor

Residence/seat of main contractor

Performed work

1)

2)

3)

4)

18. Financial information based on annual reports after your last application for the issue or extension of the permit for processing state secrets

Year

Balance sheet total

Profit

Loss

II. Contact with foreign states

19. Contacts with official authorities of foreign states and financial interests

Mark an "x" in the appropriate box (the answer must pertain to the period following your last application for the issue or extension of a permit for processing state secrets).

Yes/No

a) Has the legal person directed by you had contacts with a representative of a government, embassy or consulate of a foreign state for any other reason than the official interests of the Republic of Estonia (with the exception of contacts concerning visa applications and crossing borders)?

b) Does the legal person directed by you have assets or financial interests in a foreign state?

c) Has the legal person directed by you had any contact with foreign intelligence services?

If you answered "yes" to any of the above questions, provide an explanation in the following table.

Letter

Period (month/year)

State, company/agency/organisation

Explanation

20. Contacts with foreign agencies, enterprises and organisations

Please specify the foreign agencies, enterprises and organisations with which the legal person cooperates or has cooperated after your last application for the issue or extension of a permit for processing state secrets.

Period (month/year)

State, company/agency/organisation

Explanation

III. Other relevant information concerning legal person

21. Violations and legal disputes

Mark an “x” in the appropriate box (the answer must pertain to the period following your last application for the issue or extension of a permit for processing state secrets).

Yes/No

1) Has the legal person directed by you been punished under misdemeanour procedure?

Respond to question a

2) Has the legal person directed by you been punished under criminal procedure?

Respond to question b

3) Does the legal person directed by you currently have or has had arrears to the Tax Board? Answer question c

4) Has the legal person directed by you violated any procurement contracts concluded for the performance of public procurement? Respond to question d

5) Has the legal person directed by you any pending civil court disputes? Respond to question e

a) Authority which imposed the punishment

Date (month/year) of imposition of punishment

Basis

Type and term/category of punishment

1)

2)

3)

b) Name of court

Date (month/year) of imposition of punishment

Type and term/category of punishment

Criminal offence committed

c) Specify the arrears

Period (month/year)

Explanation

Imposed sanctions

- 1)
- 2)
- 3)
- d) Public procurement (agency, object)

Period (month/year)

Explanation

Imposed sanctions

- 1)
- 2)
- 3)
- 4)
- e) Name of court

Content of summations and/or number of case

Counterparty (counterparties) of dispute

- 1)
- 2)
- 3)

22. Financial obligations

Mark an "x" in the appropriate box (the answer must pertain to the period following your last application for the issue or extension of a permit for processing state secrets).

Yes/No

- 1) Has the legal person directed by you acquired or transferred immovable property, including common ownership (including buildings, parts thereof and apartments which are to be entered in the land register)? Answer question a
- 2) Has a right of security been established with regard to the property of the legal person directed by you? Answer question b
- 3) Does the legal person directed by you have financial obligations which exceed the average one month's turnover during the preceding financial year? Answer question c
- 4) Does the legal person directed by you have obligees who have exceeded the term for performance of their obligations (payment, etc) for more than three months? Answer question d

a) Description of immovable property

Address of location of immovable

Name of immovable property

Cadastral code of the cadastral unit

1)

2)

3)

4)

5)

b) The time (month/year) of creation and duration of right of security

Holder of right of security (business name/name, seat)

Object of right of security

Claim secured by right of security

1)

24

2)

3)

4)

5)

c) 1) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

2) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

3) Nature of financial obligation:

Bank or other person who gave the loan:

Amount of loan and interest rate:

Amount of monthly reimbursement:

Term of loan:

d) Nature of proprietary obligation

Business name/name of obligee

Size of financial obligation in kroons

IV. Other circumstances or explanations

23. In addition to the processing permit, do you also need an certificate for access to classified information of foreign states?

If yes, please specify the issuer of the classified information of a foreign state and the level of classified information of a foreign state to which you need a certificate for access:

24. Other circumstances or explanations which you consider significant:

(date, month, year) (signature, name and position of legal person)

Rein Lang
Minister of Justice

Annex 11 to Government of the Republic Regulation No. 262 of 20 December 2007
"Procedure for Protection of State Secrets and Classified Information of Foreign States"

Written consent by applicant for the issue or extension of legal person's permit to access state secrets

Business name/name:

Commercial registry code/personal identification code:

I hereby give _____

(the name of the agency conducting the security check)

permission to obtain information concerning

_____ (name of the legal person/self-employed person) from natural persons, legal persons and the agencies and bodies thereof in order to decide on the grant or extension of a permit for processing state secrets, as well as during the period of validity of the processing permit.

Please assist the person presenting this letter in every way. This information is needed for the performance of the lawful duties of the agency conducting the security check and is intended only for internal use.

(signature of the head of the legal person, or the signature of the self-employed person)

(name and office of signatory)

(day, month, year)

Rein Lang
Minister of Justice

Annex 12 to Government of the Republic Regulation No. 262 of 20 December 2007
"Procedure for Protection of State Secrets and Classified Information of Foreign States"

Confirmation by legal person to maintain state secrets made known thereto

I, _____

(name of legal person, given name, surname and position of the head of the legal person)

confirm that I am aware of the requirements concerning the protection of state secrets, the liability for violation of such requirements and the obligation to maintain the state secrets which become known to a legal person.

I have been explained that if I fail to perform the above obligation or the obligations arising from the Classified Information of Foreign States Act or legislation issued on the basis thereof or perform them in an inadequate manner, I will be held liable in the case and pursuant to the procedure provided by law.

The obligation to maintain state secrets remains in force also after the permit for processing state secrets is revoked or expires.

(date, month, year) (signature of head of legal person)

Rein Lang

Minister of Justice