Text consolidated by Valsts valodas centrs (State Language Centre) with amending regulations of:

8 February 2005 [shall come into force from 12 February 2005];

16 January 2007 [shall come into force from 19 January 2007];

13 February 2007 [shall come into force from 23 February 2007];

26 June 2007 [shall come into force from 29 June 2007];

15 September 2008 [shall come into force from 1 October 2008];

10 July 2012 [shall come into force from 18 July 2012];

4 December 2012 [shall come into force from 12 December 2012];

30 July 2013 [shall come into force from 2 August 2013].

If a whole or part of a paragraph has been amended, the date of the amending regulation appears in square brackets at the end of the paragraph. If a whole paragraph or sub-paragraph has been deleted, the date of the deletion appears in square brackets beside the deleted paragraph or sub-paragraph.

Republic of Latvia

Cabinet

Regulation No. 21

Adopted 6 January 2004

**Regulations Regarding the Protection of Official Secrets and the Classified Information of the North Atlantic Treaty Organisation, European Union and Foreign Authorities**

*Issued pursuant to*

*Section 6, Paragraph three, Section 7, Paragraphs two, four, and eight, Section 11 , Paragraph four, and Section 15, Paragraph two of the law On Official Secret*

**I. General Provisions**

1. This Regulation prescribes a uniform regime for the protection of official secrets and the classified information of the North Atlantic Treaty Organisation (hereinafter – NATO), European Union, and foreign authorities at State and local government authorities and procedures for the classified registry, use of special designations and codes, and also procedures for the supervision of the secrecy regime and internal investigation.

*[8 February 2005]*

2. Requirements of this Regulation shall also apply to merchants (commercial companies) which, while fulfilling State and local government orders, become subjects of the official secret or NATO or European Union classified information. The State or local government contracting authority, upon awarding a State or local government order which is related to an official secret or NATO or European Union classified information, shall provide in the contract for the fulfilment of the order that the contractor is liable for the conformity with this Regulation.

3. The Cabinet shall determine the special procedures by which a draft policy planning document, draft legal enactment, or informative report which in accordance with the law On Official Secret are official secret objects shall be submitted to and examined by the Cabinet.

**II. Registration, Issuance, Revoking, and Change of the Category of Personnel Security Clearances for Access to Official Secrets and Certificates**

4. The personnel security clearance for access to the official secret (hereinafter – the personnel security clearance) (Annex 1) shall certify the right of the persons who hold appropriate positions (hereinafter – the person) to have access to official secrets. The personnel security clearance shall be issued to the persons by the State security institutions prior to commencing work with official secret objects.

*[13 February 2007; 26 June 2007]*

5. The person has the right to become acquainted with NATO or European Union classified information if the position of the person is included in the list of positions for the fulfilment of which, due to the nature of the work to be done, access to NATO or European Union classified information is required and if the person has received a certificate for work with NATO and/or European Union classified information (hereinafter – the certificate). The list of positions for the fulfilment of which, due to the nature of the work to be done, access to NATO or European Union classified information is required (except for access to information which has been given to Latvia by a foreign country, international organisation or its authority and which is classified as *RESTRICTED*) shall be approved by the head of the authority. The list of positions shall be agreed upon with the subsidiary body of the Constitution Protection Bureau – the National Security Authority.

6. The National Security Authority shall perform security vetting of the persons regarding the right to access NATO or European Union classified information, issue certificates, and compile information regarding the persons who have received the certificates. The original certificates shall be stored in the National Security Authority. A copy of the certificate shall be sent for storage to the place of work (service) of the person.

7. The certificate shall be issued only to the persons who have received the personnel security clearance of the relevant category.

8. [15 September 2008]

8.1 A citizen of the Republic of Latvia who requires access to NATO or European Union classified information in relation to work in NATO or European Union institutions shall, prior to commencing the work, personally submit to the National Security Authority a submission signed by the head of the respective NATO or European Union institution for the issuance of the certificate to the aforementioned person, as well as the information referred to in Paragraph 11 of this Regulation (for security vetting). The justification for the issuance of the certificate, the time period for which the certificate is to be issued, and the information classification level shall be indicated in the submission.

*[8 February 2005]*

9. The person who has received the certificate shall become acquainted with NATO or European Union classified information only to such extent as is necessary for the fulfilment of work or service duties or the performance of a specific task.

10. The personnel security clearance shall be issued by:

10.1. the Constitution Protection Bureau – Category one personnel security clearances for access to top secret official secret objects (violet colour);

10.2. the State security institution which has vetted the person – Category two personnel security clearances for access to secret official secret objects (red colour) and Category three personnel security clearance for access to confidential official secret objects (blue colour);

10.3. [26 June 2007].

*[13 February 2007]*

11. In order to receive the personnel security clearance, the person at his or her place of work shall:

11.1. complete the questionnaire in his or her own hand (Annex 2). The questionnaire shall be completed once in five years, unless a competent State security institution has requested the submission of a new questionnaire;

11.2. certify by signing the questionnaire that he or she has been warned that the information indicated in the questionnaire shall be vetted and has become acquainted with the laws and regulations governing official secrets;

11.3. submit a *curriculum vitae* if the person is initially applying for access to official secret objects, and two photographs (3 x 4 cm).

*[26 June 2007]*

11.1 Within the scope of vetting, the State security institution shall interview the persons who are applying for access to top secret official secret objects, European Union top secret classified information, and NATO confidential, secret and top secret classified information. The persons who are applying for access to secret and confidential official secret objects, European Union secret and confidential information, need to be interviewed if the answers to questions given in the questionnaire should be clarified or important information which has been discovered during the vetting should be evaluated. The course of the interview shall be documented in writing or by an audio recording or video recording.

*[8 February 2005]*

11.2 [26 June 2007]

12. The person, prior to receiving the personnel security clearance, shall sign a non-disclosure agreement (Annex 3) on the non-disclosure of official secrets. The non-disclosure agreement shall be submitted to:

12.1. the State security institution which took the decision to issue the personnel security clearance (hereinafter – the relevant State security institution) if it issues the personnel security clearance to the person;

12.2. the structural unit for ensuring the secrecy regime if the relevant State security institution has sent the personnel security clearance to the authority or to a territorial unit authorised by the head of the authority.

*[26 June 2007]*

13. The materials of the vetting, the questionnaire, and the non-disclosure agreement of the person shall be stored by the relevant State security institution.

*[26 June 2007]*

14. The relevant State security institution shall keep a record of the personnel security clearances issued and send information to the Constitution Protection Bureau regarding the issued personnel security clearances.

*[13 February 2007; 26 June 2007]*

15. If the category of the personnel security clearance of the person needs to be changed or it needs to be reissued or revoked, the head of the authority or the head of the territorial unit of the relevant authority authorised by him or her shall submit a written submission to the relevant State security institution. The person shall submit the personnel security clearance against a signature to the structural unit ensuring the secrecy regime. The State security institution shall revoke the personnel security clearance received and, if necessary, issue a new one. Three months prior to the end of the term of validity of the personnel security clearance, the person to whom the personnel security clearance has been issued shall inform the structural unit ensuring the secrecy regime thereof.

*[16 January 2007; 26 June 2007]*

15.1 [26 June 2007]

16. If the personnel security clearance is lost:

16.1 its holder shall, without delay, inform the structural unit ensuring the secrecy regime of the fact of the loss and submit a written explanation thereto on the circumstances of the loss;

16.2. after receipt of the submission of the person on the loss of the personnel security clearance, the structural unit ensuring the secrecy regime shall carry out an internal inspection and shall send the inspection materials to the relevant State security institution. The relevant State security institution shall decide on the issuance of a new personnel security clearance or refusal to issue it. The internal inspection materials shall be appended to the official secret vetting file of the person;

16.3. [26 June 2007].

*[13 February 2007]*

17. If the circumstances referred to in Section 9, Paragraph three of the law On Official Secret are discovered or it is established that the person has knowingly provided false information regarding himself or herself, the National Security Authority shall revoke the certificate and inform the head of the authority thereof.

*[8 February 2005]*

**III. Measures for the Protection of Official Secrets and NATO or European Union Classified Information**

18. In each specific authority, the head of the authority shall be generally responsible for ensuring the measures for the protection of official secrets and NATO or European Union classified information. The head of the authority shall:

18.1. establish a structural unit for ensuring the secrecy regime which organises the ensuring of the secrecy regime in the authority and is responsible for it, and, if necessary, shall authorise the head of the territorial unit of the authority to organise ensuring of the secrecy regime at the relevant territorial unit;

18.2. in authorities which have a small volume of classified registry (up to 250 official secret objects per year), the head of the authority himself or herself shall organise the ensuring of the secrecy regime or shall assign an employee who shall organise the ensuring of the secrecy regime in the authority and shall be responsible for it;

18.3. establish a department or appoint an individual employee by a written order which shall be responsible for keeping the classified registry in the authority, and, where necessary, shall authorise the head of the territorial unit of the authority to establish a department or to appoint an employee by a written order which shall be responsible for keeping the classified registry in such territorial unit;

18.4. establish a structural unit or appoint an individual employee by a written order which shall be responsible for the circulation of NATO and/or European Union classified information;

18.5. approve the procedures for the organisation of classified registry in the authority;

18.6. approve the measures for the protection of official secret objects, NATO and/or European Union classified information in the authority;

18.7. determine or delegate the right to the head of the structural unit to determine the access of subordinate employees to a specific official secret object according to the list of official secret objects (hereinafter – the list of objects);

18.8. determine the holder (holders) of official secret objects, NATO and/or European Union classified information who shall be responsible for the implementation of the measures for the protection of a specific official secret object, NATO or European Union classified information;

18.9. be responsible for the training of holders of official secret objects, NATO and/or European Union classified information and ensuring of the relevant premises, workplace, necessary equipment, and inventory;

18.10. after receipt of the relevant written submission, decide on the issue of access of employees of other authorities to the official secret object, NATO or European Union classified information in his or her authority or the issuance thereof to employees of other authorities. If the head of the authority has grounds to believe that the submission of the employee of another authority is not related to his or her official (service) duties or specific work (service) task, the head of the authority shall, prior to issuing of the official secret object, NATO or European Union classified information, request additional information and verification for the justification of the submission from the head of the authority of the relevant employee. The requester may contest the decision of the head of the authority on the refusal to issue the official secret object, NATO or European Union classified information at the relevant State security institution or, where the issue of NATO or European Union classified information has been refused, at the National Security Authority;

18.11. approve the evacuation plan for official secret objects, NATO or European Union classified information in an emergency situation or state of emergency. The following shall be indicated in the plan:

18.11.1. the official secret objects, NATO or European Union classified information which must be delivered to the place of evacuation or must be destroyed;

18.11.2. the employees who shall be responsible for the recording and storage, preparation for transportation, guarding, or destruction of the official secret objects, NATO or European Union classified information to be evacuated;

18.11.3. the procedures by which the official secret objects, NATO or European Union classified information shall be guarded at the place of evacuation;

18.12. ensure that employees are, at least once a year, informed of the security requirements in the field of the protection of official secret objects, NATO or European Union classified information, liability for the failure to comply with the security requirements, and unsanctioned disclosure or loss of information. In cooperation with the State security institution, the head of the authority shall, at least once a year, inform employees of the possible intelligence and counter-intelligence measures which may be directed against them. Employees shall confirm the receipt of information with their signature;

18.13. agree with the National Security Authority upon and approve the list of positions referred to in Paragraph 5 of this Regulation;

18.14. issue an instruction for the protection of the official secret objects, NATO or European Union classified information if the location, size, type of use of the official secret object, NATO or European Union classified information or other circumstances preclude the fulfilment of the requirements referred to in this Regulation. The instruction shall be agreed upon with the competent State security institution or the National Security Authority.

*[8 February 2005; 16 January 2007; 10 July 2012]*

18.1 The head of the territorial unit of the authority authorised by the head of the authority shall:

18.1 1. himself or herself organise the ensuring of the secrecy regime or appoint an employee by a written order who shall organise the ensuring of the secrecy regime in the relevant unit;

18.1 2. determine the holder (holders) of the official secret objects in the relevant unit who shall be responsible for the implementation of the specific measures for the protection of the official secret objects;

18.1 3. be responsible for the training of holders of the official secret objects and the ensuring of relevant premises, workplace, necessary equipment, and inventory;

18.1 4. after receipt of a relevant written submission, decide on the access of employees of other authorities to the official secret object in his or her territorial unit or the issue thereof to employees of other authorities. If the head of the territorial unit of the authority has grounds to believe that the submission of the employee of another authority is not related to his or her official (service) duties or specific work (service) tasks, the head of the territorial unit of the authority shall, prior to issuing the official secret object, request additional information and verification for the justification of the submission from the head of the authority of the relevant employee. The requester may contest the decision of the head of the territorial unit of the authority on the refusal to issue the official secret object at the relevant authority. The requester may contest the decision of the head of the authority on the refusal to issue the official secret object at the State security institution.

*[16 January 2007]*

19. A structural unit for ensuring the secrecy regime or an employee who is responsible for ensuring the secrecy regime shall be directly subordinate to the head of the authority or – in the relevant territorial unit – to the head of the relevant unit authorised by the head of the authority. If one employee ensures the secrecy regime in the authority, all the rights and duties specified in this Regulation for the structural unit for ensuring the secrecy regime shall apply to him or her.

*[16 January 2007]*

20. A structural unit for ensuring the secrecy regime has the following duties:

20.1. to control how officials and employees who work with official secret objects, NATO or European Union classified information (hereinafter – the employee) comply and fulfil the obligations for the protection of official secret objects, NATO or European Union classified information;

20.2. to request from employees explanations regarding the failure to comply with the measures for the protection of official secret objects, NATO or European Union classified information and to notify the head of the authority of the established violations;

20.3. in the case of the loss of a personnel security clearance, to ensure the carrying out of an internal inspection regarding the fact of the loss and sending of the inspection results to the relevant State security institution;

20.4. to accept the set of the documents referred to in Paragraph 11 of this Regulation from persons who are applying for access to official secret objects and to check whether the person has provided answers to all the questions indicated in the questionnaire and has signed the questionnaire;

20.5. together with an employee of the Personnel Department to verify the conformity of the information indicated in the *curriculum vitae* and the questionnaire of the person with the personal documents at the disposal of the authority (for example, education documents and other documents) and to make a written notation on the questionnaire regarding the verification;

20.6. to send a covering letter signed by the head of the authority or the head of the territorial unit authorised by the head of the authority to the relevant State security institution for the performance of the check, appending the set of the documents referred to in Paragraph 11 of this Regulation;

20.7. to send the supplements to the data indicated in the questionnaire submitted by the person to the relevant State security institution;

20.8. to send the non-disclosure agreement signed by the person to the relevant State security institution.

*[26 June 2007]*

21. The employee who works with the official secret object, NATO or European Union classified information have the following obligations:

21.1. to stop actions of other persons due to which the official secret object, NATO or European Union classified information may be disclosed to unauthorised persons, and to notify without delay the structural unit for ensuring the secrecy regime and the head of the authority thereof;

21.2. to comply with the rules for the use, recording, and storage of official secret objects, NATO or European Union classified information;

21.3. upon issuing the official secret object, NATO or European Union classified information, to ascertain that the person has the personnel security clearance or certificate of the relevant category for work with NATO and/or European Union classified information;

21.4. prior to termination of work relations, to hand over the official secret object, NATO or European Union classified information in sufficient time to the structural unit which is responsible for the organisation of classified registry or to submit a report on the existence of the official secret object, NATO or European Union classified information prior to beginning his or her leave of absence;

21.5. upon a request of an employee of the structural unit for ensuring the secrecy regime, to present for examination without delay all the official secret objects, NATO or European Union classified information, registration and record documents;

21.6. to notify in writing the structural unit for ensuring the secrecy regime or the competent State security institution of changes in the data indicated in the questionnaire within a month.

*[26 June 2007]*

22. The official secret objects, NATO and European Union classified information may be created, compiled, stored, processed, used, forwarded, received, and destroyed electronically if a closed electronic communications network or a separately standing electronic device (hereinafter – the information system) is being used. The information system must be protected against access by unauthorised persons. The premises in which the information system is installed must conform to the security requirements which are set out for premises where official secret objects, NATO or European Union classified information are stored. The information system may not be connected to public networks, including the Internet. Prior to commencing work, the information system must be registered with the National Security Authority and must receive therefrom an accreditation certificate for the conformity of the information system with the security requirements.

*[8 February 2005; 26 June 2007]*

23. The information systems in which official secret objects, NATO and European Union classified information are processed and stored may be interconnected, using encryption systems recognised by the National Security Authority, if separate accreditation has been obtained from the National Security Authority. The National Security Authority shall determine the encryption systems which may be used for the protection of official secret objects, NATO or European Union classified information, as well as shall undertake the recording, procurement, and administration of all encryption materials. All encryption materials shall bear the special label “KRIPTO”. Access to encryption materials may be acquired only after receipt of an encryption permit.

*[8 February 2005; 26 June 2007]*

23.1 The Cabinet shall issue instructions regarding the procedures by which the security vetting, registration, and accreditation of information systems, issue of encryption permits, and distribution, storage, and recording of encryption material shall be performed, as well as regarding the security requirements which are set out for the information systems in order to ensure the processing, storage, and transfer of official secrets, NATO or European Union classified information.

*[8 February 2005]*

24. A security administrator of the information system appointed by a written direction (order) of the head of the authority or the head of the territorial unit of the relevant authority shall be responsible for the operation of the information system in which official secret objects, NATO and European Union classified information are processed and stored. The employees who service the information system must have the personnel security clearance of the relevant level which conforms to the classification level of the official secret processed and stored in the information system. If NATO and European Union confidential or secret classified information is processed and stored in the information system, the employees who service the information system must also have a certificate of one classification level higher than the classification level of the NATO and European Union classified information processed and stored in the information system. If NATO and European Union top secret classified information is processed and stored in the information system, the employees who service the information system must have a certificate which certifies their right to access NATO and European Union top secret classified information.

*[8 February 2005; 16 January 2007]*

25. The premises in which activities with official secret objects, NATO or European Union classified information are performed shall be controllable and ensured against unauthorised entry of unauthorised persons. The guard post of the authority shall, on the basis of a request from an employee, issue one-off access passes for visits to the authority and shall note in writing (given name, surname, position, authority, time) the arrival and departure of the visitor at and from the authority or the part thereof where work with official secret objects, NATO or European Union classified information is done. A visitor may visit the premises in which work with official secret objects, NATO or European Union classified information is done only in the company of an employee of the authority. If necessary, guards may be placed outside of the premises in which issues related to official secret objects, NATO or European Union classified information are discussed. A person may become acquainted with top secret official secret objects, NATO or European Union top secret classified information only in the premises in which classified registry is kept. The top secret official secret objects, NATO or European Union top secret classified information shall be appended by a list of those officials who have become acquainted with the abovementioned information and have certified this fact with their signature, and also have indicated the time and date of becoming acquainted.

26. The premises in which official secret objects, NATO or European Union classified information are accumulated shall conform to the following requirements:

26.1. the walls shall be made of:

26.1.1. certified, fireproof materials or articles (for example, reinforced concrete, fibre-reinforced concrete, concrete, lightweight concrete, reinforced concrete panels, stone, bricks, clay building blocks, expanded clay blocks, silicate blocks) the bulk density (density) of which is not less than 650 kg/m3. If the monolithic concreting technology is used in the construction of the wall, its compressive strength may not be lower than 10 MPa. If the wall is made of individual materials, the compressive strength of such materials may not be less than 5 MPa and such cement mortar and cement-lime mortar the compressive strength of which is not less than 10 Mpa shall be used for their connection, or other methods of enduring connection of the materials stipulated by the manufacturer shall be used. If materials with cavities are used for the making of the walls, during construction of the wall they must be filled up with concrete or cement mortar the compressive strength of which is not lower than 10 MPa (the requirement does not apply to perforated bricks and clay building blocks). In order to ensure the shear strength of the wall and its potential endurance against intrusion, the constructive minimum width of the wall without sound-proofing must be:

26.1.1.1. 150 mm if the wall is reinforced and its bulk density exceeds 2400 kg/m3;

26.1.1.2. 200 mm if the bulk density of the wall exceeds 2000 kg/m3 (except for the case referred to in Sub-paragraph 26.1.1.1 of this Regulation);

26.1.1.3. 250 mm if the bulk density of the wall is between 1200 and 1999 kg/m3;

26.1.1.4. 300 mm if the bulk density of the wall is between 650 and 1199 kg/m3;

26.1.2. certified level, even, or corrugated steel or stainless steel cold-rolled or hot-rolled plates which have been welded together throughout the perimeter and the minimum thickness of which is not less than 8 mm, if the entire contact length of the plates have been welded with steel or stainless steel struts (for example, T, U, I profiles, angles, rectangular or square pipes) which have been securely attached to the covering and the ceiling structure;

26.1.3. certified fireproof materials or articles (for example, autoclaved aerated concrete blocks, expanded clay blocks, gypsum blocks, double frame partition walls with two layers of plaster board plates and mineral wool sound-proofing) the bulk density of which is not less than 650 kg/m3 or the compressive strength of the materials of which is less than 5 MPa, if a steel structure (mesh) created from rods welded together at points of intersection (the gap between the rods does not exceed 200 mm, and a fitting or rod iron the diameter of which is not less than 18 mm or a square the edge of which is not less than 16 mm has been used for making of the rods) has been inserted inside the structure throughout the height of the wall. The steel structure of each wall must be welded together with the structure of the adjacent wall or its immobility must be ensured otherwise (for example, by cementing or walling in into the adjacent wall if it has been built in accordance with the conditions of Sub-paragraph 26.1.1 of this Regulation);

26.2. if the width of the wall is less than the width referred to in Sub-paragraphs 26.1.1.1, 26.1.1.2, 26.1.1.3, and 26.1.1.4 of this Regulation, the steel structure referred to in Sub-paragraph 26.1.3 of this Regulation must be built into the wall;

26.3. sound-proofing in accordance with the requirements of the Latvian construction standards shall be ensured for the walls. For the wall structures referred to in Sub-paragraphs 26.1.1, 26.1.2, and 26.1.3 of this Regulation the weighted apparent sound reduction index R’w of the internal delimiting structures of the building may not be less than 56 dB;

26.4. vertical niches, shafts, and pipelines shall not be built in the walls;

26.5. the covering shall be made of certified fireproof materials or articles (for example, reinforced concrete, reinforced concrete panels, concrete, steel structures, stone, solid bricks) the bulk density of which is not less than 1700 kg/m3. The normalized impact noise level index L’n,w of the covering structure in accordance with the requirements of the Latvian construction standards may not exceed 56 dB;

26.6. the entry door (except for the cases referred to in Sub-paragraph 26.7 of this Regulation) shall be made of:

26.6.1. steel structures;

26.6.2. air-dried (moisture less than 18 %) solid wood (for example, hornbeam, beech, ash, oak, maple) of hardness class I–III, if the the thickness of door wing is not less than 25 mm. If the thickness of door wing is 25–37 mm, they shall be covered from the outside with a steel plating of 2 mm in thickness;

26.6.3. air-dried (moisture less than 18 %) solid wood (for example, birch, pine, fir, alder) of hardness class IV–V, if the thickness of door wing is not less than 37 mm. If the thickness of door wing is 3750 mm, they shall be covered from the outside with a steel plating of 2 mm in thickness;

26.7. the entrance door to the premises where the separate record-keeping is managed, as well as to the premises of the sub-register office and of the check-point offices shall be made of steel structures;

26.8. the mechanical strength and sound isolation indicators of the door or overlight glazing (for example, wire glass, armoured glass) of the door referred to in Sub-paragraphs 26.6.2 and 26.6.3 of this Regulation shall not be lower than the indicators for the basic materials of the relevant door;

26.9. if the doors are made of steel structures, the door jamb shall be well fixed into the wall, welding it to metal pins which have been worked into the wall in the depth of at least 80 mm (the distance between the pins shall not exceed 700 mm), or the door jamb shall be welded to steel struts which have been securely fixed into the wall. The strength for the door jamb referred to in Sub-paragraphs 26.6.2 and 26.6.3 of this Regulation and its structural fixture in the wall shall be not lower than the strength of the basic materials of the relevant door;

26.10. the gap between the wings of double winged doors shall be covered from both sides with interface mouldings. It is prohibited to use doors which open in both directions and sliding doors;

26.11. the door hinges may be:

26.11.1. placed on the inside of the doors;

26.11.2. built into the door wing and frame (invisible hinges);

26.11.3. placed on the outside of the doors, if security studs which preclude removal of the doors have been immured above the hinges and below them into the wall or hammered into the door frame;

26.12. the solid wood door shall be equipped with at least one heavy duty burglar-proof lock built into the door wing. The bolt of the lock must be protected against sawing off. The distance from the front plate of the lock to the strike plate shall not exceed 5 mm. The lock shall be assembled with a profile cylinder of corresponding quality which is secured against violent unlocking, boring, and removal. To prevent the profile cylinder from being taken hold of and pulled out with pliers, it shall not be protruded for more than 2 mm beyond the cover plate. If technically possible, the door may be equipped with the lock referred to in Sub-paragraph 26.13 of this Regulation;

26.13. the door which is made of steel structures shall be equipped with a multi-point lock which locks the door in 3 or 5 points with stable steel bolts or door latches which hook into the strike plate of the lock. In addition, the door may be equipped with the locks referred to in Sub-paragraph 26.12 of this Regulation;

26.14. if traces of violent opening are visible on the lock, it must be changed without delay;

26.15. the windows shall be equipped:

26.15.1. from the outside or inside – with steel grates or metal (aluminium, steel) blinds. The steel grates shall be made of a fitting or rod iron the diameter of which is not less than 18 mm, or a steel square the edge of which is not less than 16 mm (the distance between the rods shall not exceed 150 mm). The grates shall be welded together at point of intersection. At least every second rod of the grate must be built into the wall in depth of at least 80 mm;

26.15.2. from the inside – with blinds, or other measures have been taken which prevent the room from being observed from the outside (except when the metal blinds referred to in Sub-paragraph 26.15.1 of this Regulation are consistently used);

26.16. the protection of venting systems and smoke flues shall be ensured to prevent unauthorised persons from accessing them;

26.17. the premises shall be equipped with a security and fire safety alarm which is able to operate also if disconnected from the mains network, and it shall be controlled from the room where security guard employees are staying. Functioning of the alarm shall be inspected continuously from the panel at the security guard premises. The National Security Authority shall determine requirements for alarm equipment. The security guard duties shall be continuously fulfilled by at least three security guard employees. The security guard employees must have special permits of at least Category three. If in relation to the fulfilment of work duties, the content of the highest level official secret object, NATO or European Union classified information has become known to a security guard employee, the relevant State security institutions or the National Security Authority shall warn him or her in writing of the non-disclosure of such information and liability therefore.

*[15 September 2008]*

27. The suitability of premises for the storage of official secret objects of a specific classification level shall be vetted, according to the competence, and a written opinion shall be provided by the relevant State security institution or the National Security Authority if NATO or European Union classified information is stored in the premises. The State security institution or the National Security Authority may become acquainted with the acceptance deeds of the work covered in order to evaluate the conformity of the construction of the premises with the requirements referred to in Paragraph 26 of this Regulation. The State security institution or the National Security Authority may allow deviations from the requirements referred to in this Regulation if they recognise that as a whole the implemented measures ensure the protection of official secret objects, NATO or European Union classified information in the particular premises.

*[15 September 2008]*

27.1 The following shall be indicated in the opinion referred to in Paragraph 27 of this Regulation:

27.1 1. the name of the institution which performed the vetting;

27.1 2. the name of the authority or the structural unit of the authority to be vetted;

27.1 3. the representatives of the authority or the structural unit of the authority to be vetted;

27.1 4. the names and numbers of the premises to be vetted;

27.1 5. the established deficiencies;

27.1 6. an indication on the permission to store official secret objects, NATO or European Union classified information in the particular premises.

*[26 June 2007]*

28. Official secret objects, NATO and European Union classified information shall be stored in safes in accordance with the following requirements:

28.1. NATO top secret (*COSMIC TOP SECRET*) classified information shall be stored in a separate safe separately from official secret objects and other NATO and European Union classified information;

28.2. European Union top secret (*TOP SECRET*) classified information shall be stored in a separate safe separately from objects of official secret and other NATO and European Union classified information;

28.3. official secret objects, as well as NATO and European Union confidential (*CONFIDENTIAL*) and secret (*SECRET*) classified information may be stored in one safe separately, with each type of classified information placed in separate compartments of the safe;

28.4. the security requirements for safes and suitability for the storage of the relevant level of official secret objects, NATO and European Union classified information shall be determined by the National Security Authority;

28.5. to each safe in which official secret objects, NATO and European Union classified information are stored a sticker must be attached with the following information:

28.5.1. the given name, surname, and telephone numbers of the employee responsible for the safe in order to ensure the possibility of contacting him or her in an emergency situation or when the safe is found open;

28.5.2. the registration number of the safe;

28.6. information regarding the measures which must be implemented with the official secret objects, NATO and European Union classified information stored in safes in emergency situations or a state of emergency shall be indicated in the evacuation plan.

29. The combinations of the safes storing official secret objects, NATO and European Union classified information, and one copy of the keys for the safe and premises together with information regarding the registration number, location of the safe and the employee (surname and position) who is responsible for the safe shall be kept in the case or envelope placed in the safe of the structural unit for ensuring the secrecy regime or the head of the authority, or the head of the territorial unit of the relevant authority, or the employee appointed by him or her who is responsible for ensuring of the secrecy regime in the relevant unit. The seal (stamp) stamp or signature of the employee responsible for the safe shall be on the closing flaps of the case or envelope. The seal or signature shall be covered with a see-through tape or other appropriate packaging material.

*[8 February 2005; 16 January 2007]*

30. The combination of the safe shall be changed:

30.1. at least once every six months;

30.2. if employment relations with the employee who is responsible for the safe are terminated;

30.3. if there are suspicions that the combination of the safe has become known to unauthorised persons.

31. At the end of working time the employee, upon leaving the premises in which official secret objects, NATO or European Union classified information are stored, shall perform the following activities:

31.1. check whether the official secret objects, NATO or European Union classified information have been placed safes, lock the safes, as well as close the windows;

31.2. make a notation in the control sheet on the performance of the checks specified in Sub-paragraph 31.1 of this Regulation, indicating the date and time. The notation made in the control sheet shall be certified with his or her signature. The control sheet shall be affixed to the inside of the entry door to the premises or to the wall inside the premises close to the door. The control sheet shall be kept for 60 days after making of the last entry. At the end of the abovementioned time period the control sheet may be destroyed;

31.3. lock the entry doors;

31.4. connect the alarm system of the premises;

31.5. transfer the premises to security guards.

32. If official secret objects, NATO or European Union classified information are stored in the premises, cleaning of the premises and other maintenance activities in the abovementioned premises shall be performed in the presence of the holder of the official secret, NATO or European Union classified information.

33. The structural unit for ensuring the secrecy regime or the specially appointed employee shall, not less than once a quarter, but a commission established with a direction (order) of the head of the authority or the head of the territorial unit of the relevant authority shall once a year check the existence of the official secret objects, NATO or European Union classified information in the authority or the relevant unit of the authority. The commission shall draw up a deed on the results of the check. The deed shall be kept for three years. The National Security Authority has the right to, without a warning, check the existence of NATO and European Union classified information in the authority and the compliance with the protection requirements. The relevant State security institution has the right to, without a warning, check the existence of official secret objects in the authority and the compliance with the protection requirements.

*[8 February 2005; 16 January 2007]*

34. If employment relations with the employee of the authority who has the personnel security clearance or certificate are terminated, or he or she has been assigned to fulfil other duties in the authority, the employee shall hand over all the official secret objects, NATO or European Union classified information at his or her disposal to the structural unit which keeps the classified registry or (with a deed of transfer and acceptance) to the person taking over the duties, and shall make an entry thereon in the registration and recording journals of the classified registry and/or in the electronic information system (hereinafter – the system).

35. In the territory and premises in which work with official secret objects, NATO or European Union classified information is performed, employees of emergency services, fire-fighters, emergency medical assistance teams, as well as operative groups (if a crime has been committed) are allowed to enter and stay therein in the presence of security guard employees or the employee who is responsible for ensuring the secrecy regime.

36. When delivering official secret objects, NATO and European Union classified information to the addressees in Latvia, the following conditions shall be conformed to:

36.1. the official secret objects, NATO and European Union classified information may delivered by:

36.1.1. the courier of the authority (confidential, secret, and top secret official secret objects, NATO and European Union confidential, secret, and top secret classified information);

36.1.2. an employee appointed by the head of the authority or the head of the territorial unit of the authority authorised by the head of the authority (confidential and secret official secret objects, NATO and European Union confidential and secret classified information);

36.1.3. the courier service of *valsts akciju sabiedrība “Latvijas pasts”* [State stock company Latvian Post] (hereinafter – the State stock company Latvian Post) (confidential, secret, and top secret official secret objects);

36.2. the official secret objects, NATO and European Union classified information shall be delivered, using service road transport, air transport, or by carrying (it is permitted to carry confidential and secret official secret objects, NATO and European Union confidential and secret classified information if it has not been prohibited by the authority or the territorial unit of the authority). It is prohibited to use public transport for the delivery of official secret objects, NATO and European Union classified information. The courier service of the State stock company Latvian Post may deliver official secret objects by train;

36.3. the courier of the authority, the employee appointed by the head of the authority or the head of the territorial unit of the authority authorised by the head of the authority, or the employee of the courier mail of the State stock company Latvian Post must have the personnel security clearance of the corresponding level and, when delivering NATO and European Union classified information, also the certificate of the corresponding level.

*[15 September 2008]*

37. When delivering official secret objects, NATO and European Union classified information to the addressees in foreign countries and from foreign countries, the following conditions shall be conformed to:

37.1. the official secret objects, NATO and European Union classified information may be delivered by:

37.1.1. diplomatic mail (confidential, secret, and top secret official secret objects, NATO and European Union confidential, secret, and top secret classified information);

37.1.2. the courier of the authority (confidential, secret, and top secret official secret objects, NATO and European Union confidential, secret, and top secret classified information);

37.1.3. an employee appointed by the head of the authority or the head of the territorial unit of the authority authorised by the head of the authority (confidential and secret official secret objects, NATO and European Union confidential and secret classified information);

37.2. the official secret objects, NATO and European Union classified information shall be delivered, using service road transport or air transport;

37.3. the courier of the authorities, the employee appointed by the head of the authority or the head of the territorial unit of the authority authorised by the head of the authority must have the personnel security clearance of the corresponding level and, when delivering NATO and European Union classified information, also the certificate of the corresponding level;

37.4. NATO and European Union classified information may be delivered by a courier of the authority to whom the National Security Authority has issued a written permission in advance. The written permission shall be issued for one year;

37.5. if NATO and European Union confidential or secret classified information is delivered by an employee appointed by the head of the authority or the head of the territorial unit of the authority authorised by the head of the authority, he or she must receive a written permission from the National Security Authority before each delivery;

37.6. the way of sending NATO or European Union top secret classified information and its route shall be agreed upon in advance with the National Security Authority in writing.

*[15 September 2008]*

38. During the transportation and delivery, the director-general of the abovementioned company shall be responsible for the official secret object transferred to the courier mail of the State stock company Latvian Post. The director-general shall determine the procedures for the acceptance, conveyance, delivery, and transfer of the consignment in accordance with the requirements laid down in this Regulation.

*[8 February 2005]*

39. The courier or employee who delivers official secret objects, NATO or European Union classified information:

39.1. is prohibited from leaving the entrusted information without personal supervision (for example, in hotels, hotel safes or baggage storage facilities, cars);

39.2. is prohibited from becoming acquainted with the contents of the entrusted information to be sent;

39.3. must convey the information so that unauthorised persons could not establish that an official secret object, NATO or European Union classified information is being conveyed, and become acquainted with its contents.

40. The head of the authority may allow an employee to take with him or her on official travel (also to foreign countries) secret and confidential official secret objects, NATO or European Union confidential classified information necessary for work in a double packaging if the employee uses service road transport or air transport. Prior to the taking of an official secret object, NATO or European Union classified information on official travel, the employee needs to:

40.1. receive a certification from the relevant Latvian authority or foreign organisation that the storage of the official secret objects, NATO or European Union classified information and the possibility to use service transport for the conveyance at the place of official travel shall be ensured;

40.2. during the conveyance, comply with the requirements laid down in Sub-paragraphs 39.1 and 39.2 of this Regulation.

*[8 February 2005]*

40.1 [15 September 2008]

41. In foreign countries, official secret objects, NATO or European Union classified information may stored:

41.1. in the premises of a diplomatic or consular mission of the Republic of Latvia which conform to the measures for ensuring protection of the official secret object, NATO or European Union classified information;

41.2. in the premises controlled by foreign countries with which the Republic of Latvia has concluded contracts for the protection of classified information.

42. Official secret objects, NATO or European Union classified information shall be sent in a double packaging. The inner and outer packaging shall be made in accordance with the requirements laid down in Chapter VI of this Regulation.

43. If an official secret, NATO or European Union classified information has become known to a person who does not have the relevant personnel security clearance or certificate, he or she has an obligation to preserve its secrecy. The relevant State security institution or the National Security Authority (in relation to NATO or European Union classified information) which has become aware of this fact shall warn such person thereof in writing. If the person who does not have the relevant personnel security clearance and certificate has become aware of an official secret, NATO or European Union classified information within the framework of civil or criminal proceedings, the person directing the proceedings has an obligation to inform thereof the relevant State security institution or the National Security Authority which shall warn the abovementioned person in writing of the obligation to preserve its secrecy.

**IV. Classification of Official Secret Objects, Amendment and Declassification of Classification Levels**

44. The conditions for the classification of official secret objects, amendment and declassification of classification levels shall not apply to NATO and European Union classified information.

45. The classification of official secret objects is the assignment of a classification level (top secret, secret, confidential) to an object based on the list of objects. If the information based on the list of objects conforms to the status of an official secret object, but the loss or illegal disclosure thereof cannot do any harm to national security, economic or political interests, the status of the information shall be specified in conformity with the Freedom of Information Law.

*[8 February 2005]*

46. The declassification of official secret objects is the removal of the classification level of the object.

47. An official secret object shall be classified by the employee who signs or approves it. Upon classifying an official secret object, the time period after the end of which it must be decided whether to preserve, amend, or remove the classification level of the relevant object shall be indicated. The classification level shall be reviewed by the employee who has signed or approved the official secret object if it is his or her official duty to be the holder of such official secret, or an employee whose official duty is to be the classifier of the official secret object at the moment when the classification level is reviewed.

*[30 July 2013]*

48. If it is decided to preserve the classification level initially specified for an official secret object or the classification level of a official secret object is changed, or it is declassified before the end of the initial time period, the decision-taker shall inform all holders of the relevant official secret object thereof in writing. The holder of the relevant official secret object shall, within 10 days, make amendments to the relevant object designations regarding the preservation, amendment, or declassification of the classification level.

49. The holder of an official secret object shall declassify an official secret object received from another authority, agreeing in writing thereon in advance with the authority which prepared the official secret object or upon receipt of a notification from the abovementioned authority on the declassification of the official secret object.

*[30 July 2013]*

50. When classifying an official secret object, the highest classification level of the classification levels indicated in the individual components of the relevant object shall be determined as its general classification level.

51. If several official secret objects with different classification levels are unified into one object, the highest classification level of the classification levels specified for the former separate objects shall be assigned thereto and the longest of the time periods for the preservation of the classification level shall be determined.

52. Each part of an official secret object may be used separately, designating each as an independent official secret object.

53. A refusal to provide information which is based on the fact that the requested information belongs to an official secret, the requester of the information, if he or she does not agree with the justification for the refusal, may contest it to the head of the authority. The refusal of the head of the authority to provide information to which the status of an official secret has been granted may be contested by the requester of the information to the Director of the Constitution Protection Bureau. The decision of the Director of the Constitution Protection Bureau may be contested in accordance with the procedures laid down in the law On Official Secret.

54. If an object conforms to the criteria of an official secret object, but is not included in the list of objects, the head of the relevant authority shall:

54.1. assign the abovementioned object a temporary classification level for a period of up to six months;

54.2. prepare and submit proposals for amendments to the list of objects according to specified procedures;

54.3. ensure the protection of the relevant object in accordance the requirements laid down in this Regulation;

54.4. revoke the temporary classification level of the object if within six months the list of objects has not been appropriately amended.

55. The individual unclassified parts of an official secret object, if separated from the classified official secret object, may be used openly.

56. Information used for training purposes which imitates official secret objects shall be deemed to be open.

56.1 The status of an official secret shall be granted to unclassified information received from subjects governed by private law if, in accordance with Section 2, Paragraph one of the law On Official Secret, it contains an official secret. The status of an official secret shall granted to the information by the employee to whom the subject governed by private law has sent the information, if he or she has the personnel security clearance of the relevant category. The employee shall make a notation on the received object regarding the assignment of the relevant classification level, use other special designations, as well as inform the subject governed by private law of the status of an official secret granted to the received object.

*[8 February 2005]*

57. The holder of NATO and European Union classified information, irrespective of the existence of a classification time period, is prohibited from arbitrarily changing the classification level, unless a written request or consent is received from the preparer of the information, except when the classification time period specified for the information has expired.

**V. Use of Special Designations**

58. Official secret objects shall be designated by placing the relevant designations in specific order (Annex 4) and appending special indication pages regarding the fact that the object has been appropriately classified: top secret – violet colour, secret – red colour, and confidential – blue colour. Where indication pages cannot be used, indication stickers shall be used.

*[8 February 2005]*

58.1 Indication pages and indication stickers shall also be appended to NATO and European Union classified information.

*[8 February 2005]*

59. Only the following information shall be provided In an indication page:

59.1. in the middle of the top and bottom edge of the page, the general classification level of the official secret object, NATO or European Union classified information (“SEVIŠĶI SLEPENI” [TOP SECRET], “SLEPENI” [SECRET], “KONFIDENCIĀLI” [CONFIDENTIAL]) shall be indicated;

59.2. in the middle of the page it shall be indicated that the relevant information is protected in accordance with the law On Official Secret.

*[8 February 2005]*

60. Indication stickers in the relevant colours shall be affixed to electronic information carriers (for example, disks, compact disks (CD-R)), tables, charts, drawings and photographs. An indication sticker shall include:

60.1. the classification level of the official secret object, NATO or European Union classified information;

60.2. the name of the authority;

60.3. the registration number and date of the official secret object, NATO or European Union classified information.

*[8 February 2005]*

60.1 On the right-hand side of the pre-text zone of the first page of the official secret object , the general classification level of the official secret object (“SEVIŠĶI SLEPENI” [TOP SECRET], “SLEPENI” [SECRET], “KONFIDENCIĀLI” [CONFIDENTIAL]) and the number of the copy shall be indicated.

*[8 February 2005]*

61. The pages of an official secret object shall be numbered, the order number of the page and after a dash – the total number of pages of the document shall be indicated with Arabic numerals in the right-hand corner of the bottom edge of each page. A notation on the justification of the classification and the time period shall be indicated on the first page of the document in the bottom right-hand side. Pages without any information shall not be numbered. An indication shall be made in the middle of such page: “Šī lappuse nav izmantota” [This page has not been used]. If written information is placed only on one side of the page, such an indication shall be placed on all unused backsides of such pages.

*[30 July 2013]*

62. In the middle of the top and bottom edge of each page of an official secret object, a notation shall be made on the classification level of the information included in the specific page of the relevant object (“SEVIŠĶI SLEPENI” [TOP SECRET], “SLEPENI” [SECRET], “KONFIDENCIĀLI” [CONFIDENTIAL]). If the particular page of the official secret object does not have information which contains official secrets, in the middle of the top and bottom edge of such page a notation “NAV KLASIFICĒTS” [NOT CLASSIFIED], “DIENESTA VAJADZĪBĀM” [FOR OFFICIAL USE] or “IEROBEŽOTA PIEEJAMĪBA” [RESTRICTED ACCESS] shall be made.

*[8 February 2005]*

63. If the classification level of an official secret object is amended or the abovementioned object is declassified, respective amendments shall be made to the designations and indications on the official secret object, and also the amendments shall be justified. On declassified official secrets objects a notation “NAV KLASIFICĒTS” [NOT CLASSIFIED], “DIENESTA VAJADZĪBĀM” [FOR OFFICIAL USE] or “IEROBEŽOTA PIEEJAMĪBA” [RESTRICTED ACCESS] shall be made.

*[8 February 2005]*

64. Based on the information contained therein, the individual components, as well as sections, paragraphs and sub-paragraphs of the text of an official secret object may have different classification levels or also have no secrecy. In such case, special abbreviated designations shall be used in the text of the official secret object before such parts for the designation of the classification level of the information contained therein: “Sevišķi slepeni” [Top secret] – (SS), “Slepeni” [Secret] – (S), “Konfidenciāli” [Confidential] – (K), but for official secrets components which do not contain official secrets – (N), “Dienesta vajadzībām” [For official use] – (DV) or “Ierobežota pieejamība” [Restricted access] – (IP). The classification level “Konfidenciāli” [Confidential] may be assigned to the name of the official secret object.

*[8 February 2005; 4 December 2012]*

64.1 [15 September 2008]

65. On the top left-hand corner of the first page of a the translation of foreign classified information, the word “Tulkojums” [Translation] shall be written and the country or international organisation from which such information was received, as well the designations of the formulator shall be used (Annex 5) and the relevant designations in the Latvian language.

*[8 February 2005]*

66. When preparing classified documents for the needs of NATO, the European Union, foreign international organisations and authorities, they shall be developed in accordance with the requirements of the abovementioned international organisation.

**VI. Classified Registry**

67. The documentation of the registration and recording, receipt, storage, issue, use, delivery, and destruction of official secret objects received and prepared in the authority or the relevant territorial unit of the authority shall be performed by the structural unit responsible for keeping the classified registry (hereinafter – the division), or in an authority with a small volume of classified registry (up to 250 official secrets objects per year) – a classified registry employee appointed by the direction (order) of the head of the authority.

*[16 January 2007]*

68. Classified registry shall be kept separately from the rest of the record-keeping of the authority by the division or by the relevant classified registry employee who is directly subordinate to the head of the authority. At the authority, the official secret objects shall be received and sent only through the division.

68.1 At the relevant territorial unit of the authority, the classified registry shall be kept separately from the rest of the record-keeping. The division or the relevant classified registry employee shall be directly subordinate to the head of the territorial unit of the authority. The relevant territorial unit of the authority shall receive and send official secret objects only through the division or the relevant classified registry employee.

*[16 January 2007]*

69. The circulation of NATO and European Union classified information in the authority shall be performed separately from the circulation of official secret objects, and the classified registry thereof shall be kept by a sub-registry bureau or control point bureau (hereinafter – the sub-registry) – in a special authority or a section established within a structural unit subordinate to the authority or an employee appointed by the direction (order) of the head of the authority, or a classified registry sub-structure which organises and controls the circulation and protection of NATO and European Union classified information. The sub-registry shall be directly subordinate to the head of the authority.

*[8 February 2005]*

70. The overall protection of NATO and European Union classified information transferred to Latvia shall be ensured by the Central Registration Bureau which shall supervise and co-ordinate the work of the sub-registries. The Central Registration Bureau is a sub-structure of the National Security Authority.

71. The Constitution Protection Bureau shall develop and the Director of the Constitution Protection Bureau shall approve instructions for the circulation of NATO and European Union classified information. The instructions shall stipulate in detail the procedures for the protection and circulation of NATO and European Union classified information in the Republic of Latvia.

72. If the authority receives NATO top secret (*COSMIC TOP SECRET*) or European Union top secret (*TOP SECRET*) classified information, the head of the authority shall appoint an employee of the sub-registry who shall be responsible for the storage, registration, and circulation of the classified information of such category in the authority.

73. The sub-registry shall ensure the fulfilment of the following requirements:

73.1. the registration and circulation of NATO and European Union classified information is performed separately from one another;

73.2. NATO top secret (“COSMIC TOP SECRET”) classified information is registered, stored (separate safe) and its circulation is performed separately from the rest of NATO classified information;

73.3. European Union top secret (“TOP SECRET”) classified information is registered, stored (separate safe) and its circulation is performed separately from the rest of European Union classified information.

74. An employee of the division (sub-registry) shall receive the consignments of the official secret object, NATO or European Union classified information addressed to the authority, verify the conformity of the address of the consignment, ascertain the state of the packaging of the consignment, open the outer packaging, compare the registration numbers of the consignment with those numbers indicated in the courier’s covering letter, and sign for the receipt of the consignment.

75. If the employee of the division (sub-registry) detects damage to the outer and inner packaging or inner packaging sealing of the consignment due to which the content of the consignment may have been disclosed, he or she shall take the following actions:

75.1. make a notation thereon in the courier’s covering letter;

75.2. draw up a statement in three copies. The nature of the damage shall be indicated in the statement. The recipient and the courier shall sign the statement;

75.3. make a relevant notation in the system for the registration and recording of the official secret objects, NATO or European Union classified information,

75.4. send the second copy of the statement referred to in Sub-paragraph 75.2 of this Regulation to the sender;

75.5. send the third copy of the statement referred to in Sub-paragraph 75.2 of this Regulation to the relevant State security institution (National Security Authority).

76. After the opening of the inner packaging of the consignment, the employee of the division (sub-registry) shall:

76.1. verify the correspondence of the official secret object, NATO or European Union classified information and the relevant numbers with the numbers indicated in the covering letter (if such exists) or indicated on the consignment;

76.2. draw up a statement in two copies and send the second copy of the statement to the sender, if it is established that the indicated official secret objects, NATO or European Union classified information are missing or if there are such official secret objects, NATO or European Union classified information which are not indicated in the covering letter or on the consignment;

76.3. divide the official secret objects, NATO or European Union classified information into groups according to their classification level;

76.4. append an appropriate indication sheet to each official secret object, NATO or European Union classified information;

76.5. register the official secret objects, NATO or European Union classified information in the registration and recording system corresponding to the classification level of the received official secrets objects or in the registration and recording system corresponding to the classification level (top secret, secret or confidential) of the received NATO or European Union classified information accordingly (Annex 6). Authorities in which the number of the received and sent official secret objects is small may register all received official secret objects in one system for the registration and recording of the received official secret objects (this condition shall not apply to NATO or European Union classified information).

*[8 February 2005]*

77. If the official secret objects, NATO or European Union classified information are delivered directly to the recipient by an employee of the sender, the recipient shall sign in the system for the registration and recording of the official secret objects, NATO or European Union classified information to be sent of the sender (Annex 7) or in a document which certifies receipt of the consignment. Documents which certify receipt shall be stored for three years after the end of the relevant calendar year.

78. On the right-hand side of the bottom edge of the first page of the cover letter of each received official secret object, NATO or European Union classified information a notation on the receipt and registration of the aforementioned object shall be made, and also the name of the receiving authority, the date of receipt, and the registration number shall be indicated.

79. In the relevant registration system, the received and registered official secret objects, NATO or European Union classified information shall, in return for a signature, be transferred for examination to the addressee or the head of the authority who may specify his or her directions and tasks for implementation in a resolution.

*[8 February 2005]*

80. After their signing and assigning of the relevant classification level, the official secret objects, NATO or European Union classified information shall be transferred to the division (sub-registry) which shall register them in the system for the registration and recording of the official secret objects, NATO or European Union classified information of the corresponding classification level to be sent. Authorities in which the number of the received and sent official secret objects is small (up to 250 object per year) may register all the processed official secret objects in one system for the number of the received and sent official of the official secret objects to be sent (this condition shall not apply to NATO or European Union classified information).

*[8 February 2005]*

81. [4 December 2012]

82. Confidential official secret objects, NATO or European Union classified information shall be copied by:

82.1. the holder of the relevant official secret object, NATO or European Union classified information, if it is done to ensure work or service interests, and the copies are in internal circulation within the authority. The head of the authority, upon approving the measures for the protection of official secret objects, NATO and/or European Union classified information in the authority, shall determine the place and the procedures by which the holders shall prepare copies of confidential official secret objects, NATO or European Union classified information. The prepared work copies shall not be registered. The copier may transfer a copy at the disposal of another employee after he or she has ascertained that this employee has the appropriate level of the personnel security clearance or certificate and the possibility to ensure the storage of the copy in accordance with the specified requirements;

82.2. the division (sub-registry) if a copy of the official secret object, NATO or European Union classified information needs to be sent to another authority, and shall number it.

*[8 February 2005]*

83. The division (sub-registry) shall copy a secret official secret object, NATO or European Union secret classified information according to the permission of the head of the authority. In the territorial unit of the authority, a secret official secret object shall be copied by the division or the relevant classified registry employee according to the permission of the head of the relevant territorial unit. Copies shall be numbered. The National Security Authority shall be informed within five working days of the copying of NATO or European Union secret classified information.

*[16 January 2007]*

84. Copies of a top secret official secret object may be prepared by the authority which has prepared the official secret object (document), or (with the permission of the head of the relevant authority) the recipient of the information. In individual emergency situations (for example, urgent operative activity measures need to be taken) when it the permission of the preparer for the copying of a top secret official secret object cannot be obtained or copies cannot be received, they may be prepared by the recipient of the information. The preparer of the top secret official secret object shall be notified without delay of the copying of the top secret official secret object, the number of copies made, and their recipient. It is prohibited to send a top secret official secret object to another authority without the permission of the authority which prepared the top secret official secret object.

*[8 February 2005]*

85. Copies of NATO or European Union top secret classified information on the basis of a submission from the head of the authority may be prepared only by the NATO or European Union Security Bureau or by the author of the information. In an emergency situation top secret information may be copied by the National Security Authority which shall, within three working days, inform the author of the information or the NATO or European Union Security Bureau thereof.

*[8 February 2005]*

86. Information regarding the prepared and numbered copies (date, copy number, transfer certification) shall be indicated by the employee of the division (sub-registry) in the system for the registration and recording of the received official secret objects, NATO or European Union classified information of the corresponding classification level or the system for the registration and recording of the sent official secret objects, NATO or European Union classified information of the corresponding classification level.

87. Extracts may be made from confidential and secret official secret object, NATO or European Union confidential and secret classified information which have been received from other institutions and it may be included in other official secret objects, preserving the classification level of the original official secret object, NATO or European Union classified information and assigning registration numbers thereto. Extracts may be made from top secret official secret objects (except for top secret NATO or European Union classified information) if permission has been received from the preparer.

*[8 February 2005]*

87.1 Translations of foreign classified information shall preserve the relevant classification levels specified for the originals and shall be assigned with registration numbers.

*[8 February 2005]*

88. Official secret objects, NATO or European Union classified information shall be sent in a double packaging. Only the receiving authority (without the surname and position of the official) and the address thereof shall be indicated on the outer packaging. The number of the consignment may be indicated on the outer packaging. The classification level of the contents of the consignment shall not be indicated on the outer packaging.

89. The relevant secrecy designations (for example, the classification level, the number of the copy), the precise address of the receiving authority and the relevant official, the sender and the address thereof, as well as the given name, surname of the packager of the consignment and the registration number of the sent document shall be indicated on the inner packaging of the official secret objects, NATO or European Union classified information. The inner packaging shall be stamped and places of fastening the packaging shall be covered with a transparent sealing tape or another material appropriate for the type of packaging.

90. In order to send a large-sized official secret object, NATO or European Union classified information, parcels, roll-type packages, sacks, boxes, or containers shall be used which shall be stamped with a sealing-wax stamp or seal, taking into account the requirements laid down in Paragraphs 88 and 89 of this Regulation.

91. If official secret objects, NATO or European Union classified information with different classification levels are sent in one packaging, the highest classification level of the official secret object, NATO or European Union classified information placed therein shall be specified on the inner packaging of the consignment.

92. The official secret objects, NATO or European Union classified information prepared for sending shall be recorded and a notation shall be made in the correspondence covering letter which has been sent by the courier service of the State stock company Latvian Post (Annex 8) or the courier of the authority. The covering letter shall be drawn up in two copies by the employee of the division (sub-registry). The consignment shall be placed in the outer packaging in the presence of the courier. The consignments together with the first copy of the covering letter shall be transferred to the courier service of the State stock company Latvian Post or the courier of the authority. In the second copy of the covering letter which shall remain in the division (sub-registry), the courier shall indicate the number of consignments accepted for delivery (in words), the date and time and certify the entry with his or her signature and imprint of a seal or stamp. After delivery of the consignment to the addressee, the courier shall return the first copy of the covering letter in which the recipient has indicated the number of accepted consignments (in words), date, time and has certified with his or her signature and imprint of a seal or stamp, to the division (sub-registry). Covering letters shall be stored for three years.

*[8 February 2005]*

93. Technical information media (for example, diskettes, optical disks, magnetic tapes) which contain an official secret, NATO or European Union classified information shall be registered in the division (sub-registry).

94. The registration and recording system must not contain erasures or blocked out entries. Each correction made must be justified, the surname of the relevant employee must be indicated, and he or she must certify the correction with his or her signature.

94.1 The division (sub-registry) shall also register, circulate and store such official secret objects, NATO and European Union classified information which has been received through the use of an information system accredited by the National Security Authority in accordance with Paragraphs 22 and 23 of this Regulation. Special record-keeping of such official secret objects, NATO and European Union classified information shall be managed in accordance with the requirements of Chapter VI of this Regulation by complying with the conditions of the security procedure instruction of the particular information system used.

*[15 September 2008]*

95. If the authority keeping classified registry is liquidated or reorganised, the official secret objects, NATO or European Union classified information shall be transferred to the authority which is the successor in rights and obligations of the authority to be liquidated or reorganised, or to a higher authority. If the successor in rights and obligations has not been determined, the official secret objects, upon an agreement with the Office of the Director General of the State Archives, shall be transferred under a deed to the Latvian State Archives, but NATO and European Union classified information – to the National Security Authority.

**VII. Destruction of Official Secret Objects, NATO and European Union Classified Information**

96. The official secret objects, NATO and European Union classified information (also their copies) received from other authorities shall be destroyed if they are not needed for work or if it is requested by the authority which prepared the relevant official secret object, NATO or European Union classified information. The official secret objects prepared and registered at the authority may be destroyed if they are not needed for work, except for one copy the storage of which after its declassification shall be coordinated with the State archives. The decision on the destruction of official secret objects, NATO or European Union classified information shall be taken by the head of the authority or the head of the territorial unit of the relevant authority.

*[30 July 2013]*

97. After receipt of a written order of the head of the authority or the head of the territorial unit of the relevant authority regarding the destruction of official secret objects, it shall be carried out by the employee of the division who is responsible for the storage, registration, and circulation of the relevant official secret object in the authority. A witness – an employee of the relevant State security institution – shall participate in the destruction process of top secret and secret official secret objects. Both officials shall certify the destruction with their signature in the destruction statement. The destruction statement shall be drawn up in two copies. Upon destroying the confidential official secret objects registered in the division and their copies, the destruction statement need not be drawn up, but a witness – the head of the authority or an employee appointed by him or her, the head of the relevant territorial unit of the authority or an employee appointed thereby – shall participate in the destruction process. After the operational needs of the authority are ensured, unregistered copies of confidential official secret objects shall be destroyed by the holders of the document. The destruction of such copies need not be documented.

*[16 January 2007]*

98. After receipt of a written order of the head of the authority regarding the destruction of NATO and European Union classified information, it shall be carried out by the employee of the sub-registry who is responsible for the storage, registration, and circulation of the relevant NATO and European Union classified information in the authority. An employee of the National Security Authority shall participate in the destruction process of NATO and European Union secret and top secret classified information. The destruction statement shall be drawn up in two copies on the destruction of NATO and European Union secret and top secret classified information. Both officials shall certify the destruction with their signatures in the destruction statement. One copy of the destruction statement shall be sent to the National Security Authority, but the other shall remain in storage in the sub-registry. Upon destroying NATO and European Union registered confidential classified information, the destruction statement need not be drawn up, but the head of the authority or an employee appointed by him or her shall participate in the destruction. Copies made for work, if they are not registered, shall be destroyed by the holder of the documents. The destruction of such copies need not be documented.

*[8 February 2005]*

99. After destruction of the official secret objects, NATO or European Union classified information, an employee of the division (sub-registry) shall make notations in the respective system for the registration and recording of the received or sent official secret objects, NATO or European Union classified information of the corresponding classification level on the destruction carried out. For confidential official secret objects, NATO or European Union confidential classified information the justification for the destruction, the date and the person who participated in the destruction (this record shall be certified by the relevant person with his or her signature) shall be indicated in the information system, whereas for top secret and secret official secret objects and secret or NATO or European Union top secret classified information – the number and date of the destruction statement. The employee of the division (sub-registry) shall certify the records with his or her signature.

*[8 February 2005]*

100. Official secret objects, NATO or European Union classified information shall be destroyed by burning, melting, chemical decomposition, or shredding so that the possibility of obtaining information from its medium or to restore it is lost. If the official secret objects, NATO or European Union classified information are destroyed by a shredder, the area of a strip of shredded paper may not exceed 30 mm.

*[15 September 2008]*

101. Destruction statements of official secret objects, NATO or European Union classified information shall be stored for five years, whereas destruction statement of top secret official secret objects, NATO or European Union classified information shall be stored for ten years after which they may be destroyed.

**VIII. Receipt, Transfer, Use, Declassification, and Destruction of Classified Information Sent from Foreign Countries**

102. Classified information from foreign countries shall be received, transferred, used, declassified, and destroyed in accordance with the provisions of international agreements.

**IX. Transfer of Official Secret Objects to Foreign Representatives within the Framework of Co-operation between the Republic of Latvia and Foreign Countries**

103. Official secret objects shall be transferred to foreign authorities within the framework of co-operation between the Republic of Latvia and foreign countries in accordance with the provisions of international agreements.

**X. Internal Investigation of the Disclosure or Loss of Official Secret Objects, NATO or European Union Classified Information**

104. If the head of the authority has a reason to believe that the disclosure of an official secret, NATO or European Union classified information or the loss of an official secret object, NATO or European Union classified information has occurred, he or she shall:

104.1. without delay report to a superior head and the relevant State security institution (National Security Authority);

104.2. not later than on the next day set up an internal investigation commission consisting of at least three persons. The internal investigation commission shall consist of representatives of the authority and the relevant State security institution (National Security Authority);

104.3. in co-operation with the relevant State security institution (National Security Authority) organise a search for the lost official secret objects, NATO or European Union classified information.

105. The internal investigation commission shall have the following duties:

105.1. to clarify the circumstances (for example, time, place) of the disclosure of official secrets, NATO or European Union classified information or the loss of the official secret object, NATO or European Union classified information;

105.2. to identify the perpetrators;

105.3. to clarify the causes and circumstances which have facilitated the committing of the violation, and to take measures for their elimination;

105.4. to specify the harm which has been caused or might have been caused in the case of disclosure of official secret, NATO or European Union classified information or the loss of the official secret object, NATO or European Union classified information.

106. Members of the internal investigation commission shall have the following rights:

106.1. to inspect the premises, territory, safes, tables, and cupboards of the relevant authority;

106.2. to inspect systems for the registration and recording of official secret objects, NATO or European Union classified information and other documents;

106.3. to request explanations from the relevant employees of the authority.

107. The internal investigation shall be carried out and an opinion shall be prepared within 15 working days. The opinion shall indicate whether a violation has been committed and who is liable for it.

*[26 June 2007]*

108. The internal investigation commission shall submit the internal investigation materials and opinion to the head of the relevant authority. The internal investigation materials shall, without delay, be sent to the Constitution Protection Bureau (National Security Authority).

109. The internal investigation materials which are related to the disclosure or loss of a confidential and secret official secret object, NATO or European Union confidential and secret classified information shall be stored for five years, but the internal investigation materials which are related to the disclosure or loss of a top secret official secret object, NATO or European Union top secret classified information – for 10 years.

*[8 February 2005]*

110. The National Security Authority shall, without delay, inform the NATO Security Bureau or the European Union Security Bureau of the unsanctioned disclosure of NATO or European Union classified information and the results of the internal investigation.

*[8 February 2005]*

111. If the lost official secret objects, NATO or European Union classified information have not been found, the search for such may be terminated if all possible search measures have been taken and the circumstances of the loss, as well as the persons at fault have been established.

112. The head of the relevant authority shall send the materials regarding the termination of the search for the official secret objects, NATO or European Union classified information to the Constitution Protection Bureau (National Security Authority).

**XI. Closing Provisions**

113. Structural units for ensuring secrecy and classified registries (also sub-registries) shall be established and their activities shall be ensured within the framework of the number of staff positions provided for in the budget and the work remuneration fund.

114. The relevant State security institution (National Security Authority) shall evaluate the conformity of the authority for the commencement of work with official secret objects, NATO or European Union classified information and shall provide a relevant opinion. The authority may commence work with official secret objects (NATO or European Union classified information) if a positive opinion has been received.

115. Up to the day of issue of the Cabinet instructions referred to in Paragraph 23.1 of this Regulation, but not later than until 1 July 2005, the instruction accepted by the National Security Authority shall be in effect.

*[8 February 2005]*

116. The designations of official secret objects, the classified registry journals, the deeds of acceptance and transfer and destruction statements on official secret objects which have been created prior to the coming into force of this Regulation shall, until the end of the specified time period of the classification, retain the assigned classification level.

117. Cabinet Regulation No. 225 of 25 June 1997, Regulations Regarding Protection of Official Secrets (*Latvijas Vēstnesis*, 1997, No. 167/168; 2000, No. 88/89; 2002, No. 159; 2003, No. 5), is repealed.

118. The premises which the relevant State security institution or the National Security Authority has recognised as appropriate for the storage of official secret objects, NATO or European Union classified information until 1 October 2008 need not be transformed in accordance with the requirements of Paragraph 26 of this Regulation.

*[15 September 2008]*

Prime Minister E. Repše

Minister for Defence Ģ. V. Kristovskis

**Annex 1**

Cabinet Regulation No. 21

6 January 2004

**Personnel Security Clearance for Access to an Official Secret (Sample)**



|  |  |
| --- | --- |
| Averss | Front |
| Institūcijas nosaukums | Name of authority |
| Fotogrāfija | Photograph |
| Vārds un uzvārds | Given name and surname |
| Reverss | Back |
| Pirmās (otrās, trešās) kategorijas | First (second, third) category |
| **ATĻAUJA** | **SECURITY CLEARANCE** |
| Pieejai sevišķi slepeniem (slepeniem, konfidenciāliem) valsts noslēpuma objektiem | for access to top secret (secret, confidential) official secrets objects |
| Nr.00001 | No. 00001 |
| Derīga līdz 00.00.0000. | Valid until 00.00.0000 |
| Valsts drošības iestādes vadītājs | Head of the National Security Authority |
| (paraksts un tā atšifrējums) | (signature and full name) |

Minister for Defence Ģ. V. Kristovskis

**Annex 2**

Cabinet Regulation No. 21

6 January 2004

**Questionnaire**

*[26 June 2007]*

After completing of the questionnaire, the information indicated therein is an official secret of level “confidential”. All columns of the questionnaire must be completed by hand. If necessary answers can be continued in an annex. Information that is known and can be ascertained must be provided in the questionnaire.

|  |  |
| --- | --- |
| 1. Given name and surname (in block letters) | 2. Previous given name and surname (date and reason for changing) |
| 3. Year and date of birth | 4. Place of birth (country, city, district, parish) |
| 5. Personal identity number **\_\_ \_\_ \_\_ \_\_ \_\_ \_\_ - \_\_ \_\_ \_\_ \_\_ \_\_** | 6. Nationality |
| 7. Citizenship, the manner of its acquisition |
| 8. Contacting possibilities |
| Home telephone | Mobile telephone | Work telephone | E-mail address |
| 9. Have you previously received a personnel security clearance for work with official secrets? (Indicate the category and the issuing body) |
| 10. Have access to official secrets been denied to you? (If it has been, indicate the reasons and circumstances for the denial in annex) |
| 11. Permanent/declared place of residence for the last 15 years |
| From | To | Address |
|  |  |  |
| 12. Places of stay (for more than three months) outside the permanent/declared place of residence during the last five years, also in foreign countries  |
| 13. Places of employment in the last 15 years, also in foreign countries |
| Name of the place of employment | Address | From | To | Position |
|  |  |  |  |  |
| 14. Military (alternative service), also in foreign countries, service in the system of the Ministry of the Interior |
| From | To | Country, armed forces, location and number of the unit, structure of the Ministry of the Interior | Position | Highest service rank |
|  |  |  |  |  |

|  |
| --- |
| 15. State and military awards, also of a foreign country |
| 16. Education, also unfinished |
| From | To | Educational institution | Acquired speciality | Acquired degree |
|  |  |  |  |  |
| 17. Foreign language skills (fluent, conversational level) |
| 18. Marital status (married, divorced, widowed, in actual cohabitation), the year of entering into marriage, the year of dissolution of marriage |
| 19. Information regarding family members and other relatives, also regarding a person with whom actually lives together, regarding step-brothers, step-sisters |
| Relationship | Given name, surname, premarital surname | Personal identity number | Nationality | Citizenship | Place of residence | Place of employment and position |
| Spouse/person with whom actually lives together |  |  |  |  |  |  |
| Father |  |  |  |  |  |  |
| Mother |  |  |  |  |  |  |
| Brothers/step-brothers |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sisters/step-sisters |  |  |  |  |  |  |
| Children |  |  |  |  |  |  |
| Father-in-law |  |  |  |  |  |  |
| Mother-in-law |  |  |  |  |  |  |
| Brothers-in-law |  |  |  |  |  |  |
| Sisters-in-law |  |  |  |  |  |  |
| 20. Information regarding persons which are not indicated in Paragraph 19 of the questionnaire, but with whom there is a joint property |
| Given name, surname | Personal identity number | Place of residence | Place of employment | Position |
|  |  |  |  |  |
| 21. Disciplinary punishments in effect | For what and when they have been imposed |
|  |  |

|  |  |
| --- | --- |
| 22. Criminal record, including in foreign countries, if the conviction has been extinguished, set aside, the person has been granted clemency or amnestied  | For what has been punished, in which court, and when |
|  |  |
| 23. Have you been held criminally liable, including in foreign countries?  | What have you been held criminally liable for, where and when |
|  |  |
| 24. Have you been a participant in criminal proceedings during the last five years? Have you been a participant in administrative or civil proceedings during the last year? | Procedural status and when |
|  |  |
| 25. Administrative punishments within the last year, also in foreign countries  | For what and what punishment |
|  |  |
| 26. Have you been deported from any country? Has entry into any country been denied to you?  | Country, date, and potential reason |
|  |  |
| 27. Have you or the persons referred to in Paragraph 19 of the questionnaire at any given time have had contact with foreign State security institutions, special services, intelligence and counterintelligence institutions, including the U.S.S.R. and L.S.S.R. State Defence Committee (given name, surname, time, type, place), also if they were related to the fulfilment of work or service duties? Has a secret cooperation been ever offered to you? |
| 28. Cases or attempts of blackmail, threats and other danger or the attempts thereof from separate persons, organisations, or authorities against you or the persons referred to in Paragraph 19 of the questionnaire |

|  |
| --- |
| 29. Have you ever consulted a medical practitioner due to the use of alcohol, narcotic, psychotropic, or toxic substances or due to disorders of mental nature? Do you use (have you used) psychotropic products or narcotic substances (which ones, for what purpose)?  |
| 30. Belonging to religious confessions, religious organisations (also non-traditional). Name and and denomination of the organisation |
| 31. Belonging to unregistered organisations and their associations (name and status) |
| 32. Belonging to political organisations (parties) and their associations within the last five years (name, status, time period) |
| 33. Indicate all professional, social, or charitable organisations in which you are or have been a member, in which you are participating or working or have participated or worked within the last five years |
| Name | From | To | Operational aims and functions |
|  |  |  |  |
| 34. Have you (your family members) ever worked for the Communist Party of the Soviet Union (Latvian Communist Party), the Latvian S.S.R. Working Peoples International Front, the Work Collectives United Council, the War and Work Veterans Organisation, or the All-Latvia Society Rescue Committee?  |
| Given name, surname | Name | Period | Status |
|  |  |  |  |
| 35. Additional income outside the primary place of employment (type, place) |
| 36. Have you ever been involved in a military conflict as a participant or as an injured person? (If you have, indicate the place, time, reason) |
| 37. Indicate the persons who are permanently residing outside countries belonging to the North Atlantic Treaty Organisation or the European Union with whom you are maintaining a regular contact |
| Given name, surname | Place of residence | Type of contacts |
|  |  |  |
| 38. Do you have at your disposal facts, information, or assumptions which may be used against you or your family members for the purposes of blackmail or discreditation? (Indicate yes or no) |

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, certify with my signature that I have become acquainted with the laws and regulations governing work with official secrets and I am informed that the information that I have provided may be verified in accordance with the procedures laid down in law. I have completed this document, indicating all information that is at my disposal and being aware that any intentional (knowingly) incorrect statements or distortion of facts is a basis for denying my access to official secrets.

I undertake to provide to the State security institution, upon a request thereof, bank information and information from other credit institutions regarding my monetary savings and financial transactions.

I undertake to notify the structural unit for ensuring the secrecy regime or the competent State security institution in writing of changes in the data indicated in Paragraphs 1, 2, 7, 8, 11, 12, 18-33, 35-38 of the questionnaire within a month.

I certify the correctness of the information provided with my signature \_\_\_\_\_\_\_\_\_\_\_\_

on \_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_

The conformity of the information indicated in the questionnaire with the documents at the disposal of the institution has been verified.

on \_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(The given name, surname, and signature of the employee of the structural unit for ensuring the secrecy regime)

**Annex 3**

Cabinet Regulation No. 21

6 January 2004

**Non-disclosure Agreement**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, undertake:

(given name, surname)

1) not disclose information which contains official secrets and which will be entrusted or will become known to me while fulfilling official (service) duties;

2) without objections and accurately fulfil the requirements of directions (orders), regulations and instructions related to conformity with the secrecy regime with which I have been acquainted;

3) report on attempts to obtain official secrets from me, as well as on violations of the secrecy regime known to me.

I have been warned that for the disclosure of an official secret, as well as the loss of official secret objects and other violations of the secrecy regime I will be held criminally and disciplinary liable in accordance with law.

\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(signature)

Non-disclosure Agreement was accepted by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(position, surname, and signature of the responsible person)

Minister for Defence Ģ. V. Kristovskis

**Annex 4**

Cabinet Regulation No. 21

6 January 2004

**Sample of the Formatting of the First Page of an Official Secret Object (Document)**

*[30 July 2013]*

Classification level of the page

Details of the form of the author of the document

|  |  |  |
| --- | --- | --- |
|  Translation |   |  Classification level of the document |
|   |   |   |
| (notation on the country or international organisation) |   |  Number of the copy |   |

Place of issuance of the document

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  Code |   |   |   |   |   |
|  Date |   |  Number |   |   |   |
|  To |   |  Number |   |  Addressee |   |
|   |  (date) |   |   |   |   |
|   |   |   |   |   |   |   |   |
|  Summary of the content |   |
|   |

Text of the document

|  |  |  |
| --- | --- | --- |
| Title of the position | Signature of the official | Given name and surname |
|   |   |   |
|   |
| Indications regarding the change of the classification level or regarding declassification |   |   | Justification of classification |   |
|   |   |
| Time period for the status of secrecy |   |
|   |   |   |   |
|   |   |   | Time for the review of the status of secrecy |   |
|   |   |   |   |
|   |   |   |
|   |   |  Notation on the receipt of the document: |
|   |   |  date and time |   |
|   |   |  registration number |   |
|   |   |   |
|   |   |  Number of the page and |
|   | Classification level of the page |  total number of pages |

**Annex 5**

Cabinet Regulation No. 21

6 January 2004

**Designations of Classified Documents of Certain Foreign Countries or International Organisations**

*[8 February 2005]*



Minister for Defence Ģ. V. Kristovskis

**Annex 6**

Cabinet Regulation No. 21

6 January 2004

**Information to be Included in the Registration and Recording Journals of the Classified Registry, and/or Electronic Information Systems Regarding the Received Official Secret Object, Regarding the Received NATO Classified Information, and Regarding the Received European Union Classified Information**

1. Date of the receipt of the document.

2. Registration number of the receipt of the document.

3. The document registration number and date assigned by the National Security Authority or the sender.

4. Sender of the document.

5. Addressee of the document.

6. Author of the document and name of the document (brief content).

7. Number of the copy.

8. Number of pages in the document and the annex.

9. Information regarding the transfer of the document or acquaintance with its contents:

9.1. the position, given name, surname of the recipient of the document, signature thereof for the receipt and date of receipt;

9.2. the given name, surname of the employee and signature thereof for the return of the document.

10. Information regarding the sending of the document:

10.1. the authority, position, given name and surname of the recipient;

10.2. the time and date of the receipt of the document, signature of the recipient;

10.3. notes on the sending.

11. Information regarding the copying of the document:

11.1. the time and date of the copying of the document, number of the copy;

11.2. the person to whom the copy was transferred or sent (position, given name, and surname);

11.3 the time of receipt of the document, given name, surname of the recipient;

11.4. justification for the destruction of the copy, the person who destroyed the copy (position, given name, surname, and signature);

11.5. notes on the destruction of the copy.

12. Information regarding the destruction of the document:

12.1. justification for the destruction of the document, the time, the person who destroyed the document (position, given name, surname, and signature);

12.2. number and date of the destruction statement.

13. General notes.

Minister for Defence Ģ. V. Kristovskis

**Annex 7**

Cabinet Regulation No. 21

6 January 2004

**Information to be Included in the Registration and Recording Journals of the Classified Registry, and/or Electronic Information Systems Regarding the Sent Official Secret Object, Regarding the Sent NATO Classified Information and Regarding the Sent European Union Classified Information**

1. Registration date of the document.

2. Registration number of the document.

3. Author of the document and name of the document (brief content).

4. Structural unit which developed the document, the given name and surname of responsible employee.

5. Number of pages in the document and the annex.

6. Addressee.

7. Number of the copy.

8. Information regarding the sending or transfer of the document:

8.1. the position, given name, surname of the recipient of the document and signature thereof for the receipt, time of receipt of the document;

8.2. the number of the document certifying the receipt of the document and date.

9. Given name, surname of the employee and signature thereof for the return of the document, date and time of the return of the document.

10. Information regarding the copying of the document:

10.1. the time and date for the copying of the document, the number of the copy;

10.2. the person to whom the copy was transferred or sent (position, given name, and surname);

10.3. the time of receipt of the document, the person who received the document (given name, surname, and signature);

10.4. justification for the destruction of the copy, the position, given name, surname, and signature of the person who destroyed the copy;

10.5. notes on the destruction of the copy.

11. Information regarding the destruction of the document:

11.1. justification for the destruction of the document, the time of destruction, the person who destroyed the document (position, given name, surname, and signature);

11.2. number and date of the destruction statement.

12. General notes.

Minister for Defence Ģ. V. Kristovskis

**Annex 8**

Cabinet Regulation No. 21

6 January 2004

**Sample of Courier Covering Letter**

*[8 February 2005]*



|  |  |
| --- | --- |
| Pavadraksts Nr. \_\_\_\_\_\_\_ sūtījuma piegādei ar kurjeru | Covering Letter No. \_\_\_\_\_\_\_\_\_\_\_ for the delivery of a consignment by courier |
| 20 \_\_\_.gada \_\_\_\_ . \_\_\_\_\_\_\_ | on \_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ |
| Valsts akciju sabiedrības “Latvijas pasts” kurjerpasts | Courier mail of the State stock company Latvian Post |
| Kurjerpasta zīmoga vieta | Place for seal of the courier mail |
| Sūtījuma veids | Type of consignment |
| Paketes | Packets |
| Pakas | Parcels |
| Izsniegts kurjeram | Issued to courier |
| Izsniegts adresātam | Issued to addressee |
| Nodots atpakaļ | Delivered back |
| Neizsniegtos sūtījumus: | Consignments not issued: |
| nodeva atpakaļ | were delivered back |
| saņēma | received by |
| **Izsniegšanas pareizību pārbaudīja** | **Correctness of issue was verified by** |
| (amats, paraksts un tā atšifrējums) | (position, signature, and full name) |
| 20 \_\_\_.gada \_\_\_\_ . \_\_\_\_\_\_\_ | on \_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ |



|  |  |
| --- | --- |
| Nr.p.k. | No. |
| Reģistrācijas numurs | Registration number |
| Nosūtītāja norādītais numurs | Number indicated by the sender |
| Nosūtīšanas vieta | Place of dispatch |
| Adresāts un adrese | Addressee and address |
| Kategorija | Category |
| Saņēma (paraksts, saņemšanas datums un laiks) | Received (signature, date of receipt and time) |
| Zīmoga vieta | Place for seal |
| Kopā pavadrakstā | In total in the covering letter |
| (skaits vārdiem) | (number in words) |
| paketes; | packets; |
| (skaits vārdiem) | (number in words) |
| pakas | parcels |
| Pavadrakstu sastādīja | The covering letter was drawn up |
| (datums) | (date) |
| (amats, paraksts un tā atšifrējums) | (position, signature, and full name) |
| Pārbaudīja | Verified |
| (datums) | (date) |
| (amats, paraksts un tā atšifrējums) | (position, signature, and full name) |
| Pavadrakstā ierakstītos | The \_\_\_\_ consignments recorded in the covering letter |
| (skaits vārdiem) | (number in words) |
| sūtījumus piegādei pieņēma | were accepted for delivery by |
| Kurjers | Courier |
| (paraksts un tā atšifrējums) | (signature and full name) |
| 20 \_\_\_.gada \_\_\_\_ . \_\_\_\_\_\_\_ plkst. \_\_\_ | on \_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ at \_\_\_\_\_\_\_\_\_\_\_\_\_ o’clock |

Minister for Defence Ģ. V. Kristovskis