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

8 March 2022 [shall come into force on 16 March 2022].

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. 508

Adopted 6 July 2021

**Procedures for Surveying Critical Infrastructure, Including European Critical Infrastructure, and for Planning and Implementation of Security Measures and Continuity of Operation**

*Issued pursuant to*

*Section 22.2, Paragraph six of the National Security Law*

**I. General Provisions**

1. The Regulation prescribes the procedures for surveying critical infrastructure, including European critical infrastructure, and for planning and implementation of security measures and continuity of operation.

2. The Regulation shall not apply to the critical infrastructure the operation of which is determined by the 1961 Vienna Convention on Diplomatic Relations and the 1963 Vienna Convention on Consular Relations.

**II. Identification of Critical Infrastructure and European Critical Infrastructure**

3. The State Security Service, the Constitution Protection Bureau, and the Defence Intelligence and Security Service shall:

3.1. identify the potential Category A, B, and C critical infrastructure and submit to the Ministry of the Interior proposals for the inclusion thereof in the aggregate of critical infrastructure;

3.2. identify the potential European critical infrastructure and submit to the Ministry of the Interior proposals for the determination thereof as a European critical infrastructure.

4. The Ministry of Defence shall, in cooperation with the sectoral ministry, identify the potential Category D critical infrastructure and submit to the Ministry of the Interior proposals for the inclusion thereof in the aggregate of critical infrastructure.

5. The State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service shall, in accordance with the competence specified in the aggregate of critical infrastructure, inform the owner or legal possessor of Category A, B, or C critical infrastructure of:

5.1. inclusion of the critical infrastructure in the aggregate of critical infrastructure;

5.2. determination of the critical infrastructure as a European critical infrastructure.

6. The sectoral ministry shall, in cooperation with the Ministry of Defence, inform the owner or legal possessor of Category D critical infrastructure of the inclusion of the critical infrastructure in the aggregate of critical infrastructure.

7. A critical infrastructure may be recognised as a European critical infrastructure, if disruption to the activity of the relevant critical infrastructure or destruction thereof would significantly affect at least two Member States of the European Union and an agreement has been reached with the relevant Member States of the European Union. The significance of such effects shall be evaluated in terms of cross-cutting criteria, including the consequences resulting from the dependence of several sectors on other types of critical infrastructure.

8. The cross-cutting criteria referred to in Paragraph 7 of this Regulation are:

8.1. casualties criterion (assessed in terms of the potential number of fatalities or injuries);

8.2. economic effects criterion (assessed in terms of the significance of economic loss or degradation of products or services, including the loss of essential services, alternatives for the provision of services and disruption of services and length of restoration thereof);

8.3. public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services, alternatives for the provision of services and disruption of services and length of restoration thereof).

9. The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular critical infrastructure.

10. The responsible ministry shall prepare and submit to the Ministry of the Interior proposals for determination of precise threshold values for each critical infrastructure which shall be applied to the cross-cutting criteria.

11. The Ministry of the Interior, on the basis of the submitted proposals, shall:

11.1. prepare and submit to the Cabinet draft legal acts regarding the aggregate of critical infrastructure and the allocation of competences of the State security institutions in ensuring the planning and implementation of security measures as regards critical infrastructure, including European critical infrastructure;

11.2. not less than once a year, prepare and submit to the Cabinet an informative report on the security situation of the critical infrastructure;

11.3. inform the European Commission and European Union Member States, which may be significantly affected by the potential European critical infrastructure, regarding such European critical infrastructure and reasons, why it was determined as the potential European critical infrastructure;

11.4. coordinate bilateral or multilateral negotiations with other European Union Member States, which may be significantly affected by the potential European critical infrastructure;

11.5. once a year, prepare information intended for the European Commission regarding the number of designated European critical infrastructures per sector and the number of European Union Member States dependent on each designated European critical infrastructure, and submit it to the Cabinet for approval;

11.6. every two years, prepare information intended for the European Commission regarding the types of threats and vulnerabilities in each European critical infrastructure sector and submit it to the Cabinet for approval.

12. Draft legal acts related to the aggregate of critical infrastructure and the allocation of competences of the State security institutions in ensuring the planning and implementation of security measures as regards critical infrastructure, including European critical infrastructure, shall be approved by the Cabinet.

13. The Minister for the Interior is entitled to establish a collegial inter-institutional working group for the fulfilment of the tasks referred to in Paragraph 11 of this Regulation and to determine the composition, tasks, rights, and agenda thereof.

**III. Planning of Security Measures for Category A, B, and C Critical Infrastructure and European Critical Infrastructure**

14. The owner or legal possessor of a critical infrastructure or a European critical infrastructure shall appoint a person responsible for the security of the infrastructure and determine the tasks thereof.

15. A person responsible for the security of a critical infrastructure or a European critical infrastructure may be a person:

15.1. who is a citizen of Latvia;

15.2. who has not been punished for an intentional criminal offence;

15.3. who has not been convicted for an intentional criminal offence, releasing from a punishment;

15.4. who has not been held criminally liable of committing an intentional criminal offence, except the case when a person has been held criminally liable but the criminal proceedings have been terminated on the grounds of exoneration;

15.5. who has not been put under guardianship;

15.6. who is not or has not been a staff employee or non-staff employee of the security service of the U.S.S.R., Latvian S.S.R. or a foreign state, or an agent, resident or safe-house keeper thereof;

15.7. who is not or has not been a participant (member) of an organisation prohibited by the laws of the Republic of Latvia, decisions of the Supreme Council or court adjudications after prohibition of such organisations;

15.8. who has received the opinion of a narcologist and a psychiatrist that he or she has not been diagnosed as having mental disorders or addiction to alcohol, narcotic, psychotropic or toxic substances;

15.9. who in accordance with the information at the disposal of the State Security Service, the Constitution Protection Bureau, the Defence Intelligence and Security Service, or the State Police, does not belong to groups of organised crime, unlawful militarised or armed formations, and also to non-governmental organisations or associations of non-governmental organisations that have commenced activities (legal) prior to the registration thereof or continue to operate after suspension or termination of the activities thereof by a court ruling;

15.10. who has work experience of at least two years in the planning or implementation of the physical security measures. This condition shall not apply to a person responsible for the security of a critical infrastructure or a European critical infrastructure who has been vetted by the State security institutions in accordance with their competence.

16. The State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service may vet employees of critical infrastructure or European critical infrastructure, and also the owner, members of the board and employees of a merchant, if the merchant provides services in the critical infrastructure, who have access to information or technological equipment important to the functioning of the critical infrastructure or European critical infrastructure, or who provide services important to the functioning of the critical infrastructure or European critical infrastructure, and evaluate information in relation to a person’s criminal record for intentional criminal offences and facts that give grounds to doubt his or her ability to retain restricted access or classified information. On the basis of the results of screening, the relevant State security institution shall provide recommendations to the owner or legal possessor of the critical infrastructure or European critical infrastructure for the performance of security measures.

17. The State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service shall, in accordance with the competence of the aforementioned State security institutions, vet and approve the nomination of the person responsible for the security of a critical infrastructure or a European critical infrastructure.

18. If according to the information at the disposal of the State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service the person does not conform to the requirements referred to in Paragraph 15 of this Regulation, the State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service shall recommend that the owner or legal possessor of the critical infrastructure or European critical infrastructure restricts access of the aforementioned person to the information or technological equipment important to the functioning of the critical infrastructure or European critical infrastructure.

19. The person responsible for the security of a critical infrastructure or a European critical infrastructure shall:

19.1. plan security measures for the critical infrastructure or the European critical infrastructure;

19.2. evaluate and determine the list of the information, technological equipment, or services important to the functioning of the critical infrastructure or European critical infrastructure which shall be submitted to the State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service in accordance with the competence of the aforementioned State security institutions;

19.3. organise theoretical and practical training in physical security for the employees involved in the provision of physical security measures for the critical infrastructure at least once a year in accordance with the procedures and to the extent determined by the owner or lawful possessor of the critical infrastructure or European critical infrastructure;

19.4. inform the State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service in accordance with the competence of the aforementioned State security institutions not later than one month prior to the day of the training referred to in Sub-paragraph 19.3 of this Regulation.

20. The information referred to in the Annex 1 to this Regulation shall be included in the documents regulating the security measures for critical infrastructure or European critical infrastructure.

21. The documents governing the security measures of critical infrastructure or European critical infrastructure shall be coordinated with the State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service according to the competence of the aforementioned State security institutions.

22. The State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service shall, in accordance with their competence, control the fulfilment of the requirements specified in the documents governing the security measures of critical infrastructure or European critical infrastructure and provide recommendations for the elimination of deficiencies established during inspections, and also as provide recommendations for the topic of the training referred to in Sub-paragraph 19.3 of this Regulation.

23. The State Security Service shall provide recommendations for enhancing the security measures of critical infrastructure or European critical infrastructure according to the specified levels of terrorism threats.

24. Security or defence plans for civil aviation objects, objects of ports and port facilities, information and communication technologies, ionising radiation objects, if they have been determined as the critical infrastructure or European critical infrastructure, shall be developed and coordinated according to the procedures specified in the laws and regulations governing the relevant sector.

**IV. Planning of the Continuity of Operation of Critical Infrastructure in Case of Threat to National Security**

25. A plan for the continuity of operation of critical infrastructure in case of threat to national security (hereinafter – the plan for the continuity of operation) shall be developed in accordance with Annex 2 to this Regulation.

26. The owner or legal possessor of critical infrastructure shall appoint a person responsible for planning the continuity of operation of critical infrastructure and determine the tasks thereof:

26.1. to prepare a plan for the continuity of operation in cooperation with the sectoral ministry and the Ministry of Defence;

26.2. to ensure regular updating of the plan for the continuity of operation in cooperation with the sectoral ministry and the Ministry of Defence.

27. The person responsible for planning the continuity of operation of critical infrastructure in Category A, B, and C critical infrastructure may also simultaneously be the person responsible for the security of the infrastructure referred to in Paragraph 14 of this Regulation.

28. The person responsible for planning the continuity of operation of critical infrastructure to whom Paragraph 27 of this Regulation does not apply may be the person who meets the requirements referred to in Sub-paragraphs 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7, 15.8, and 15.9 of this Regulation.

29. The State Security Service, the Constitution Protection Bureau, or the Defence Intelligence and Security Service shall, in accordance with the competence of the said State security institutions, vet and approve the nomination of the person responsible for planning the continuity of operation of a critical infrastructure.

30. If the aggregate of critical infrastructure includes infrastructure for which continuity of operation has already been established in civil protection plans, plans for overcoming threat to national security, or disaster medicine plans or which has a system for ensuring the continuity of operation that has been certified by an external audit and complies with international standards, or if those criteria are applied to critical infrastructure after the date of entry into force of this Regulation, a new plan for the continuity of operation shall not be developed, but the owner or legal possessor of the critical infrastructure shall appoint a person responsible for the continuity of operation of the critical infrastructure and the aforementioned person shall, if necessary, supplement the existing plans for the continuity of operation in cooperation with the sectoral ministry and the Ministry of Defence.

31. If the aggregate of critical infrastructure includes several objects and systems of a single legal person, a single comprehensive plan for the continuity of operation shall be developed for that legal person.

32. The owner or legal possessor of critical infrastructure shall submit a self-assessment to the Ministry of Defence and the sectoral ministry on the updating of the plan for the continuity of operation at least every four years or, in case of significant changes, within one year at the latest. The sectoral ministry may, in cooperation with the Ministry of Defence, at any time evaluate the plan for the continuity of operation on a sample basis and, if necessary, recommend changes therein.

**V. Implementation of Security Measures for Critical Infrastructure and European Critical Infrastructure**

33. The implementer of the provision of the physical security measures of Category A critical infrastructure shall be determined by an individual Cabinet order.

34. The implementation of the physical security measures of Category B and C critical infrastructure shall be ensured by the owner or legal possessor of the critical infrastructure.

35. The Cabinet may determine that the implementation of physical security measures for a certain Category B critical infrastructure or European critical infrastructure is ensured by the units of the State Police or the National Armed Forces.

35.1 In order to effectively implement the security and protection measures of the critical infrastructure or European critical infrastructure, the owner or legal possessor of critical infrastructure or European critical infrastructure may, upon concluding a cooperation agreement with the National Armed Forces, agree on the establishment of a subunit of the National Guard at the critical infrastructure or European critical infrastructure.

[*8 March 2022*]

36. It is prohibited to make video recordings, take photographs, or otherwise document an object of Category A, B, and C critical infrastructure or European critical infrastructure without prior agreement with the owner or legal possessor thereof, provided that an information sign “BEZ SASKAŅOŠANAS FOTOGRAFĒT, FILMĒT AIZLIEGTS” (“NO PHOTOGRAPHY OR VIDEO RECORDING WITHOUT PERMISSION”) is placed at the relevant object of critical infrastructure or European critical infrastructure (Annex 3).

37. In case of declaring an energy crisis, a high and critically high terrorism threat level, an emergency situation or a state of exception, the Cabinet may decide that the National Armed Forces or the State Police take over complete or partial ensuring of measures for the physical security of a certain Category B, C, and D critical infrastructure or European critical infrastructure.

38. In the case of the declaration of a high and critically high terrorism threat level, an emergency situation associated with terrorism and public disorder, a state of exception or state of war, an owner or legal possessor of critical infrastructure or European critical infrastructure shall coordinate his or her actions with the State Police, the National Armed Forces, and the State Security Service, the Constitution Protection Bureau or the Defence Intelligence and Security Service according to the competence of the State security institutions specified in laws and regulations, taking into account the location of the relevant critical infrastructure and other specific factors.

**VI. Closing Provisions**

39. Cabinet Regulation No. 496 of 1 June 2010, Procedures for the Identification of Critical Infrastructure, Including European Critical Infrastructure and Planning and Implementation of Security Measures (*Latvijas Vēstnesis*, 2010, No. 97; 2013, No. 122; 2017, No. 114), is repealed.

40. The owner or legal possessor of critical infrastructure shall develop a plan for the continuity of operation by 1 June 2023.

41. The Ministry of the Interior shall prepare a draft legal act regarding the aggregate of critical infrastructure and submit it to the Cabinet within three months after the date of entry into force of this Regulation.

42. For critical infrastructure for which, at the moment of coming into force of this Regulation, continuity of operation has already been established in civil protection plans, plans for overcoming threat to national security, or disaster medicine plans or which has a system for ensuring the continuity of operation that has been certified by an external audit and complies with international standards, a new plan for the continuity of operation shall not be developed, but the owner or legal possessor of the critical infrastructure shall appoint a person responsible for the continuity of operation of the critical infrastructure and the aforementioned person shall, if necessary, by 1 June 2023 supplement the existing plans for the continuity of operation in cooperation with the sectoral ministry and the Ministry of Defence.

**Informative Reference to European Union Directives**

The Regulation contains legal norms arising from Directive 2008/114/EC of the European Council of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Prime Minister A. K. Kariņš

Deputy Prime Minister, Minister for Defence A. Pabriks

**Annex 1**

Cabinet Regulation No. 508

6 July 2021

**Mandatory Information to be Included in Documents Regulating the Security Measures of Category A, B, and C Critical Infrastructure or European Critical Infrastructure**

1. General information regarding the critical infrastructure or the European critical infrastructure – name, owner or lawful possessor, location (address) of the critical infrastructure or the European critical infrastructure, purpose of the document.

2. The institution (structural unit) that ensures the implementation of security measures.

3. Security of external perimeter (for example, fencing and the layout thereof, lighting and the layout thereof, video surveillance and alarm systems).

4. Control of admission to the critical infrastructure or the European critical infrastructure or the territory thereof (for example, admission points, the layout thereof, working hours, the regime of permits for employees, visitors, vehicles and cargoes, and samples of personal identification documents).

5. Restricted access areas (for example, the layout thereof, admission points, control of admission for employees, visitors and vehicles).

6. Functions of the security personnel (for example, the location, duties, rights, patrolling regime).

7. The video surveillance systems and the layout thereof of the critical infrastructure or the European critical infrastructure.

8. The alarm systems for the physical security of the critical infrastructure or the European critical structure.

9. Planning of the critical infrastructure or the European critical infrastructure.

10. Actions in dangerous situations (explosion, armed attack, discovery of an explosive object, receipt of information regarding threats of explosion, receipt of a suspicious postal consignment, unauthorised access or attempt thereof, unauthorised making of video recordings, taking of photographs, or other documentation of a critical infrastructure or European critical infrastructure).

11. Plan for the continuity of operation in case of threat to national security.

Deputy Prime Minister, Minister for Defence A. Pabriks

**Annex 2**

Cabinet Regulation No. 508

6 July 2021

**Guidelines for Developing a Plan for the Continuity of Operation of Critical Infrastructure in Case of Threat to National Security**

1. The guidelines lay down the minimum requirements and procedures for planning the continuity of operation of critical infrastructure in case of threat to national security.

2. According to the specifics of the sector, deviations from individual points of the guidelines may be permitted subject to separate agreement with the relevant sectoral ministry and the Ministry of Defence.

3. The owner or legal possessor of critical infrastructure, including European critical infrastructure (hereinafter – the critical infrastructure), shall, in cooperation with the relevant sectoral ministry and the Ministry of Defence, develop a plan for the continuity of operation of critical infrastructure in case of threat to national security (hereinafter – the plan). The plan shall specify:

3.1. the critical services and the minimum scope thereof to be provided at least at the defined level during threat to national security;

3.2. the critical personnel and their responsibilities, and also the measures for the preparation of the personnel;

3.3. the facilities necessary for operation (infrastructure, technological equipment, and necessary materials and technical means, resources and raw materials, other facilities);

3.4. algorithms for action during a crisis.

4. The minimum requirements for the continuity of critical services to be ensured during a threat to national security shall be determined individually in cooperation with the sectoral ministry and the Ministry of Defence and shall be included in the plan. The plan shall:

4.1. describe critical functions and processes;

4.2. define the scope of critical services to be provided at the defined level;

4.3. define the maximum permissible duration of interruption in the provision of critical services beyond which it is impossible to continue the provision of the respective critical service;

4.4. define the required restoration time and priorities for the restoration and continuation of critical functions.

5. With regard to human resources for ensuring critical functions, the owner or legal possessor of the critical infrastructure shall:

5.1. evaluate and determine the necessary critical personnel, including support personnel, to ensure the continuity of provision of critical services and processes. During a state of exception declared in case of threat to national security, critical personnel shall not be subject to mobilisation, but their obligation is to continue working. The owner or legal possessor of the critical infrastructure shall prohibit the critical personnel from termination of employment;

5.2. inform critical personnel of their status and responsibilities by laying it down in the employment contract and job description or by a separate order issued by the institution (for example, regarding critical personnel), or otherwise, and also provide the training or preparation of critical personnel;

5.3. establish procedures for replacing or reinforcing critical staff, including procedures in case certain critical personnel are not available;

5.4. if the situation permits, adapt infrastructure and allocate resources in advance to allow for shift work, overnight stays or prolonged stays of the personnel in working premises;

5.5. determine the channels of communication and internal communication (including the means of communication to be used) to notify and inform critical personnel.

6. The infrastructure logistics shall provide for relocation to alternative working premises (alternative location) if routine working premises are not available. For this purpose, the owner or legal possessor of the critical infrastructure shall, if possible, evaluate the specific characteristics of the particular object of critical infrastructure and:

6.1. identify, in advance, suitable infrastructure (alternative location) located at least 50 kilometres from the existing infrastructure and suitable for ensuring the critical functions (minimum required: communications support, if the situation permits – alternative energy solutions, availability of water);

6.2. develop procedures for the relocation (temporary or permanent) of personnel and technological equipment to the alternative working premises, by identifying in advance the required number of transport units and other logistics support (including for the accommodation, deployment of personnel);

6.3. identify opportunities to mobilise personnel, equipment and materials and technical means available at the alternative location by defining the requirements in advance.

7. With regard to the technological equipment (hereinafter – the equipment) and materials and technical means required for the provision of critical services, the plan shall provide for:

7.1. a list of critical equipment and materials and technical means;

7.2. identification of alternatives to critical equipment and materials and technical means, options for substitution;

7.3. equipment for ensuring continuity in case of loss or failure of equipment and materials and technical means;

7.4. actions for repairing, restoring, upgrading equipment or creating alternatives (including replacement of providers of outsourced services);

7.5. timely back-up of digital systems and equipment to ensure access to data, systems and processes also from the alternative location;

7.6. the impact of the security of supplies with regard to the continuity of operation of equipment (availability of support personnel, availability of spare parts, repairs);

7.7. backup power supply for information systems and the provision of an autonomous power supply system;

7.8. ensuring the continuity of the provision of the critical service by alternative methods and means if no information systems ensuring the provision of the critical service are located in the territory of Latvia.

8. It is recommended not to use technologies manufactured by companies whose reputation in the European Union and NATO Member States is questioned due to suspicions of privacy violations, unauthorised acquisition of non-public information, or threats to national security.

9. With regard to transport required for the provision of critical services (if applicable), the plan shall identify:

9.1. the transport required for the provision of critical services;

9.2. alternatives;

9.3. the availability of drivers and specialists, and the possibilities of substitution;

9.4. fuel supply.

10. The plan shall reflect:

10.1. electronic communications and voice telephony equipment and databases thereof (including access from alternative working premises, alternative or backup communications and data transmission systems);

10.2. power supply facilities, alternatives and the impact of outsourcing;

10.3. availability of natural gas and petroleum products (alternatives);

10.4. heating, water supply, availability of sewerage (alternatives);

10.5. logistics solutions and alternatives thereof (unavailability of transport).

11. The resource (supply) system shall provide for the availability and supply of resources (for example, identification of critical raw materials) required for the specific nature of operation of the critical infrastructure in case of threat to national security, including an assessment of the security and continuity aspects of supply and timely identification of alternative supply chains or alternatives to critical raw materials, including possible locations thereof.

12. Information regarding identified shortages of critical raw materials and materials, unavailability of materials and technical means and other identified vulnerabilities, together with the self-assessment of critical infrastructure, shall be submitted to the relevant sectoral ministry.

13. The plan shall address issues of security and resilience of supplies:

13.1. identification of at least Tier 1 suppliers and their geographic placement to identify vulnerabilities in situations of disruptions in international supply chains and allow timely identification of possible alternatives;

13.2. distribution of supply risks (multi-vendor suppliers), avoiding dependence on a single foreign supplier;

13.3. involvement in supply chains of high-risk suppliers whose reputation in the European Union and NATO Member States is questioned due to suspicions of privacy violations, failure to respect human rights, unauthorised acquisition of non-public information or threats to national security shall be discouraged;

13.4. from the point of view of security and resilience of supplies, local supply chains and local manufacturers, processors and service providers shall be given preference.

14. The plan shall reflect algorithms for action during a crisis:

14.1. provide for the provision of critical services within the defined scope in case of threat to national security;

14.2. provide procedures for contacting personnel in case of threat to national security (define communication and internal communication, notification and information);

14.3. establish the procedures for activation and operation of the crisis management team during a crisis, and also the coordination mechanism with the sectoral ministry;

14.4. establish a crisis communication protocol (internal, external);

14.5. establish the procedures for a flexible and rapid reaction to incidents by implementing crisis management procedures and protocols.

15. The priority of the company’s operation shall be the provision of critical services within a defined scope and all available internal resources of the company shall be dedicated to this. In case of disruption in provision of critical services, all resources shall be devoted to restoring the defined functions and operational processes, as far as possible minimising the losses caused, by rapidly implementing restoration scenarios or relocating and continuing operations from the alternative location.

16. Suspension of operation is only permitted:

16.1. if permission or other tasks are received from the authority responsible for overcoming the threat;

16.2. in situations when the lives of personnel are threatened and this threat cannot be eliminated, even by relocating to the alternative location.

17. The plan may also identify the support required from State authorities to ensure the performance of critical functions in case of threat to national security:

17.1. priority provision of energy, gas and petroleum products;

17.2. provision of communications;

17.3. physical security;

17.4. logistics support;

17.5. other support according to an assessment provided by the sectoral ministry and the Ministry of Defence.

18. The plan shall provide for the testing and self-assessment of the system for the continuity of operation, including the organisation of training in cooperation with the relevant sectoral ministry and the Ministry of Defence at least every four years.

19. The plan and amendments to the plan shall be approved by the owner or legal possessor of the critical infrastructure.

Deputy Prime Minister, Minister for Defence A. Pabriks

**Annex 3**

Cabinet Regulation No. 508

6 July 2021

**Sample of the Information Sign**

1. The information sign “BEZ SASKAŅOŠANAS FOTOGRAFĒT, FILMĒT AIZLIEGTS” shall constitute a white rectangle in black frame with a stylised pictogram of video recording and photography equipment and an inscription in the Latvian language.



2. Background of the information sign shall be white, 210 x 297 mm (picture). The middle of the information sign shall show a stylised pictogram of video recording and photography in black. The prohibition sign shall be in a round shape, sides of the sign and the diagonal line crossing the pictogram from the left to the right at 45° shall be red (the red part shall account for at least 35 % of the square of the sign). Diameter of the prohibition sign – 14 cm. The text of the information sign “BEZ SASKAŅOŠANAS FOTOGRAFĒT, FILMĒT AIZLIEGTS” shall be arranged in four rows. The height of the letters above the pictogram shall be 12 mm, the height of the letters under the pictogram – 17 mm. The inscription in the Latvian language in black letters “TĀLRUNIS:” shall be on the bottom left-hand side of the information sign (the height of the letters – 5 mm) together with a place where the owner or lawful possessor of a critical infrastructure or European critical infrastructure indicates the contact telephone number of the relevant critical infrastructure or European critical infrastructure.

3. The information sign shall be in the following colours (colour requirements have been specified in accordance with the PANTONE, CMYK, and RGB systems):

3.1. the rectangle and also the background of the pictogram of video recording and photography equipment – in white (PANTONE 663C or C0 M0 Y0 K0, or R255 G255 B255);

3.2. the stylised pictogram of video recording and photography equipment and the inscription “BEZ SASKAŅOŠANAS FOTOGRAFĒT, FILMĒT” – in black (PANTONE NEUTRAL BLACK C or C0 M0 Y0 K100, or R35 G31 B32);

3.3. the contour of the prohibition sign and the inscription “AIZLIEGTS” – in red (PANTONE 485C or C0 M100 Y100 K0, or R237 G28 B36);

3.4. the frame of the information sign – in black (PANTONE NEUTRAL BLACK C or C0 M0 Y0 K100, or R35 G31 B32).

4. Procedures for using the sign:

4.1. when erecting the sign on the spot one of the following sizes shall be selected:

4.1.1. 148 x 210 mm;

4.1.2. 210 x 297 mm;

4.1.3. 297 x 420 mm;

4.2. the size of the information sign in polygraphically printed publications shall be selected according to the used scale but not less than 148 x 210 mm by preserving proportions of a rectangle;

4.3. in other cases not referred to in Sub-paragraphs 4.1 and 4.2 of this Annex signs of different sizes may be used by preserving proportions of a rectangle.

Deputy Prime Minister, Minister for Defence A. Pabriks