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

19 December 2017 [shall come into force on 1 January 2018];

15 January 2019 [shall come into force on 18 January 2019];

11 August 2020 [shall come into force on 18 August 2020];

7 March 2023 [shall come into force on 15 March 2023].

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. 442

Adopted 28 July 2015

**Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements**

*Issued pursuant to*

*Section 8, Paragraphs five and six of the Law on the Security of Information Technologies and Section 4, Paragraph two of the Law on State Information Systems*

[*15 January 2019*]

**I. General Provisions**

1. The Regulation prescribes:

1.1. the minimum security requirements for the information and communication technologies of the State and local government authorities, and the procedures by which the State and local government authorities and the owners or lawful possessors of the critical infrastructure of information technologies ensure conformity of the information and communication technologies systems to the minimum requirements;

1.2. general security requirements for the State information systems;

1.3. security requirements for information technologies on legal persons governed by private law that are the operators of essential services and digital service providers.

[*15 January 2019*]

2. This Regulation shall not apply to the information and communication technologies systems where the processing or storage of the official secret, classified information of the North Atlantic Treaty Organisation (hereinafter – the NATO), the European Union and foreign institutions or the information for service needs.

[*19 December 2017*]

3. This Regulation shall apply to the information and communication technologies systems of the State and local government authorities or the critical infrastructure of information technologies, including the State information systems (hereinafter – the systems) in the testing stage, and also the systems delivered for use. Adequate protection of the information present in the system shall be ensured in other stages of the system (planning, designing and development).

[*15 January 2019*]

4. The duties of the person responsible for the security management of the information technologies referred to in this Regulation in respect of the State information system shall be performed by the security manager of a system, whereas in respect of the critical infrastructure of information technologies – the person responsible for infrastructure security.

[*15 January 2019*]

4.1 State and local government authorities shall use such information and communication technologies in their activities that conform to the requirements laid down for systems in this Regulation and also take into consideration the recommendations developed by the competent State security institution and the Information Technologies Security Incidents Response Institution regarding the information and communication technologies to be used (including regarding free software and security measures to be taken).

[*15 January 2019*]

4.2 Legal persons governed by private law that are the operators of essential services and digital service providers comply with the requirements laid down for systems in this Regulation insofar as it is not provided for otherwise in this Regulation.

[*15 January 2019*]

5. A set of measures is taken for the security of a system in order to:

5.1. ensure availability of the information (access to the information in a certain period after requesting thereof);

5.2. ensure integrity of the information (preserving of full and unchanged information);

5.3. ensure confidentiality of the information (delivery of information only to the persons authorized to receive and use it);

5.4. protect the information resources of the system (files, including those containing the information stored in the system, processed and available to the system users, and the documentation of the system);

5.5. protect the technical resources of the system (computers, software, data carriers, computer network equipment and other technical equipment ensuring the system operation);

5.6. establish certain threats to security of the system (an action performed with an intent (deliberately) or as a result of negligence, or an event that may make changes, damages, destruction of the information or technical resources, or their getting into possession of unauthorised persons, or as a result whereof the access to the resources may be interrupted or impossible);

5.7. assess the security risk of the system;

5.8. detect the security incident of the system;

5.9. restore the operation of the system after a security incident of the system.

5.1 The State and local government authority, except for the diplomatic and consular missions of the Republic of Latvia abroad, shall store data in a Member State of the NATO, European Union, or European Economic Area and direct Internet traffic within the territory of the NATO, European Union, and European Economic Area if data exchange takes place within the territory of the NATO, European Union, and European Economic Area.

[*7 March 2023*]

6. The systems are divided in two categories – basic and increased security systems.

7. In order to place the system of State and local government authorities that is not the information system of the critical infrastructure or the system which is used for the provision of the essential service and the digital service in the category of basic or increased security system, the person responsible for the security management of information technologies (hereinafter – the responsible person) shall assess it in accordance with the following methodology:

7.1. evaluate the acceptable level of risks referred to in Sub-paragraph 13.5 of this Regulation and assign the appropriate security (accessibility, integrity and confidentiality) category:

7.1.1. if unplanned interruption of the service ensured by the system within the intended working time of the system may exceed 24 hours a month (summed up time), the system is assigned the accessibility category C;

7.1.2. if unplanned interruption of the service ensured by the system within the intended working time of the system may not exceed 24 hours a month (summed up time) but it may exceed four hours (in total) a month, the system is assigned the accessibility category B;

7.1.3. if unplanned interruption of the service ensured by the system within the intended working time of the system may not exceed four hours a month (summed up time), the system is assigned the accessibility category A;

7.1.4. if the threat to integrity of the data stored in the system does not create a risk for ensuring basic functions of the State and local government authority, the system is assigned the integrity category C;

7.1.5. if the threat to integrity of some data stored in the system creates a risk for ensuring basic functions of the State and local government authority, the system is assigned the integrity category B;

7.1.6. if the threat to integrity of the data stored in the system creates a risk for ensuring basic functions of the State and local government authority, or the threat to integrity of some data stored in the system could endanger the national interests and basic values of the Republic of Latvia or lead to a catastrophe, the system is assigned the integrity category A;

7.1.7. if the system contains only publicly available information, or unauthorised disclosure or leaking of the information stored in the system does not create a risk for the State and local government authority, the system is assigned the confidentiality category C;

7.1.8. if restricted access information is processed in the system, except for sensitive personal data, or unauthorised disclosure of the information stored in the system or the only consequences of leaking thereof are possible damage to the reputation of the State and local government authority, other authorities or the Republic of Latvia, the system is assigned the confidentiality category B;

7.1.9. if sensitive personal data are processed in the system, or unauthorised disclosure of the information stored in the system or the leaking thereof could cause more significant consequences than damage to the reputation of the State and local government authority, other authorities or the Republic of Latvia, the system is assigned the confidentiality category A;

7.2. if the system is assigned three security categories B or at least one security category A, the system shall be considered as an increased security system;

7.3. in any other cases, the system shall be considered as a basic security system.

[*15 January 2019*]

7.1 The information systems of the critical infrastructure and the systems which are used for the provision of the essential service or the digital service accordingly by the operator of essential services or the digital service provider shall be recognised as increased security systems.

[*15 January 2019*]

8. The State and local government authority, the owner or lawful possessor of the critical infrastructure of information technologies, the operator of essential services or the digital service provider (hereinafter – the authority) shall draw up the following documents for each system and also shall ensure the monitoring and control of the fulfilment of requirements stipulated therein:

8.1. security policy of the system;

8.2. internal security regulations of the system;

8.3. provisions for use of the system;

8.4. security risk management plan of the system;

8.5. restoration plan of the system operation.

[*15 January 2019*]

9. The requirements referred to in Sub-paragraphs 8.2, 8.3, 8.4 and 8.5 of this Regulation shall not be applicable to basic security systems.

10. The document referred to in Sub-paragraph 8.1 of this Regulation shall be approved by the head of the authority, whereas the documents referred to in Sub-paragraphs 8.2, 8.3, 8.4, and 8.5 of this Regulation shall be approved by the head of the authority or an authorised person thereof. The authority shall, at least once a year, review all documents referred to in Paragraph 8 of this Regulation, and also in the following cases:

10.1. if the changes to the system may affect security of the system;

10.2. if the threats to security of the system have changed or new threats have been detected;

10.3. if a number of the incidents to security of the system suddenly increase or a significant incident to security of the system has occurred;

10.4. if the changes to the organisational structure of the authority affect the organisation of security management of the system;

10.5. if any amendments to the laws and regulations governing the operation of the system are made.

[*11 August 2020*]

11. If the authority controls or uses more than one system, each document referred to in Paragraph 8 of this Regulation may be designed as a uniform document for several or all controlled or used systems, by indicating the specific requirements for each system, where necessary.

12. Conformity of the security measures of the system with the requirements referred to in Paragraph 5 of this Regulation is evaluated based on the results of the security inspection of the system. If significant deficiencies are established during this inspection, the authority shall carry out measures for rectification thereof in accordance with the requirements referred to in the Law on the Security of Information Technologies.

12.1 The head of the State and local government authority shall, upon concluding the contract for the development, introduction, or maintenance of information and communication technologies systems, determine the responsible person who shall supervise the development, introduction of information and communication technologies systems and the performance of the outsourcing contract for maintenance.

[*11 August 2020*]

**II. Security Policy of the System and Procurement Requirements**

13. The security policy of the system shall include:

13.1. objectives and guidelines for the security policy of the system;

13.2. characterisation and analysis of the system in the security field;

13.3. the principles for organisation of the security management of the system;

13.4. conformity of security of the system to the laws and regulations and standards;

13.5. security principles of the system, acceptable level of security risk of the system (accessibility, integrity and confidentiality risk) in conformity with the methodology referred to in Paragraph 7 of this Regulation and other security criteria of the system (for example, time of continuous operation of the system, time for restoration of the system operation, conditions based on which the daily procedures are replaced with the crisis management procedures).

14. The authority shall ensure that the information referred to in Paragraph 13.5 of this Regulation is available to registered system users.

[*19 December 2017*]

15. The following shall be taken into account when developing the security policy of the system:

15.1. the system users performing the system administration activities use special user accounts (hereinafter – account of the system administrator) not used for performance of daily activities;

15.2. each registered user account is linked to a certain natural person. If the accounts not linked to a certain natural person are used in the system (hereinafter – the system accounts), control mechanisms preventing a possibility for registered users to use the system accounts must be incorporated in the system;

15.3. if multi-factor authentication is not used in the system, i.e. one attribute without a static nature (for example, code calculator, single use SMS code) and at least one other attribute, registered system users must definitely use the passwords;

15.4. the length of the password of the system user is not less than nine characters and contains at least one capital letter of the Latin alphabet and a small letter of the Latin alphabet and also a number or a special symbol;

15.5. the passwords of the system user are prohibited to be stored electronically and transported in a decoded way, including also within the scope of the user authentication process, except for the case referred to in Sub-paragraph 15.7 of this Regulation;

15.6. the password of the system user is not fully displayed to the user during entering thereof;

15.7. the password of the system user sent in the public data transmission network in a decoded way is used only once and valid for a period not exceeding 72 hours after sending thereof;

15.8. the functionality allowing the system user to store his or her password in a way that it does not need to be entered the next time when login takes place is not allowed in the system;

15.9. the default passwords (set up by the manufacturer or distributor) are not used for the equipment including the infrastructure equipment ensuring the system functioning;

15.10. creation and storage of the system audit trail (hereinafter – system trails) are ensured at least six months after making an entry. The system trails shall contain information on connection to or disconnection from the system, data selection and also the creation, alteration or deletion of an account, recording the time of the event which corresponds to the coordinated universal time (UTC) of the actual event, Internet Protocol address wherefrom the activity was carried out, description and also information on the initiator of the activity – identifier, connection metadata;

15.11. any access to the system is traceable to a certain account of the system user or internet protocol (IP) address;

15.12. available software updates are installed on the system, prior to that evaluating the necessity thereof;

15.13. anti-virus functionality is included in all equipment of the end users in the possession of the authority used on daily basis for connecting to the system;

15.14. the system functionality shall be carried out with minimum possible rights;

15.15. the systems which ensure the receipt of electronic mail from external resources process the incoming message at least according to the requirements of e-mail authentication protocol (DMARC), implementing e-mail processing in accordance with the DMARC policy of the sender domain name, generation and sending of a report to the point of contact specified in the DMARC configuration;

15.16. the authority which is the electronic mail domain owner publishes a DMARC compliant entry in the domain name system (DNS) thereof, indicating a strict reject policy (p=reject), has a procedure in place for the receipt of DMARC messages and analysis thereof;

15.17. the authority ensures creation of backup copies and recovery of the data stored in the information systems.

[*19 December 2017; 15 January 2019; 11 August 2020 / Sub-paragraphs 15.15 and 15.16 shall come into force on 1 January 2021. See Paragraph 45*]

16. Stricter security requirements than laid down in this Regulation may be provided in the security policy of the system insofar as it is not in contradiction with other laws and regulations.

17. An authority prior to developing or starting a procurement on development of a new system shall develop and approve the security policy of this system and ensure compliance therewith during the development stage of the system.

18. An authority shall ensure that intrusion tests are performed prior to accepting a new system into operation. The intrusion tests shall be performed by a legal person or the staff of the authority not participating in development of the system.

19. An authority shall ensure the security test of the system referred to in Paragraph 12 of this Regulation by performing an examination of the fulfilment of the requirements of the security documentation at least once a year.

20. If an outsourcing agreement with a service provider is signed for the maintenance of the system in the institution, the performance of the agreement shall be supervised by the responsible person, and security requirements not lower than those referred to in this Regulation shall be included in the agreement. The following information shall be provided for in the agreement:

20.1. description of the outsourced service to be received;

20.2. precise requirements in respect of the volume and quality of the outsourced service;

20.3. rights and obligations of the authority and provider of the outsourced service, including:

20.3.1. the rights of the authority to constantly supervise the quality of the provision of the outsourced service;

20.3.2. the rights of the authority to give instructions to be performed mandatory to the provider of the outsourced service in the matters related to honest, high quality, timely and complying with the laws and regulations performance of the outsourced service;

20.3.3. the rights of the authority to submit a justified written request to the provider of the outsourced services to immediately terminate the outsourcing agreement if the authority has established that the provider of the outsourced services fails to fulfil the requirements laid down in the agreement regarding the volume or quality of the outsourced service;

20.3.4. the obligation of the provider of the outsourced service to ensure a possibility for the authority to constantly supervise the quality of the provision of the outsourced service;

20.3.5. the obligation of the provider of the outsourced service to immediately report on a security incident of information technologies and to take all the necessary measures for the prevention thereof;

20.3.6. the obligation of the provider of the outsourced service to inform of the sub-contractor and conformity thereof with the security requirements laid down in this Regulation and the contract;

20.4. security inspections of the system laid down in laws and regulations and identified by the head of another authority;

20.5. access requirements for data and storage thereof and also the obligation of the supplier to delete all data at the disposal thereof after expiry of the contract, except for the case if the contract is concluded repeatedly with the same service provider on the same subject-matter of the contract.

[*11 August 2020*]

21. If the State and local government authority commences a procurement regarding improvements to an existing system, it shall ensure that the relevant security requirements are included in the procurement specification.

[*15 January 2019*]

22. If the State and local government authority commences a procurement on the development of a new system, it shall include the requirements in the procurement specification, providing for the following:

22.1. the specific period of maintenance and provision of support to the system (including for rectification of security flaws of the system);

22.2. delivery of the software source code of the system and the rights to use it for the authority not later than after the period referred to in Sub-paragraph 22.1 of this Regulation, and also after making any amendments or improvements thereto;

22.3. a possibility to continue using the system during the period referred to in Sub-paragraph 22.1 of this Regulation with the most recent versions of the software (for example, operating system, database management system, interpreter) mandatory for the functioning of the system.

[*15 January 2019*]

23. By carrying out a procurement regarding the development of a new system or improvements to an existing system, the State and local government authority shall include a prohibition in the procurement specification to restrict in the agreement the rights laid down in Section 29, Paragraph one of the Copyright Law.

[*15 January 2019*]

23.1 When purchasing a service, software, or equipment, the State and local government authority shall include in the procurement specification and in the contract the obligation of the service provider and the product manufacturer to inform, during the term of the contract, of or to publish information on the disclosed vulnerabilities related to the information and communication technologies product or service, their prevention measures and deadlines.

[*11 August 2020*]

23.2 When concluding a procurement contract for the purchase of routers, switches, external firewalls, intrusion detection systems, anti-intrusion systems, antivirus software, and also for services, software, or equipment that provide protection and monitoring functions of basic security systems, the State and local government authority shall ensure conformity with the requirements specified in Paragraph 36.1 of this Regulation. When concluding a framework agreement, the provisions thereof shall include a reference to the restrictions specified in Paragraph 36.1 of this Regulation which shall apply to the conclusion of procurement contracts within the framework of agreement for the purchase of goods or services referred to in this Paragraph.

[*11 August 2020*]

**III. Requirements for the Increased Security Systems**

24. When developing the security policy of the system for the increased security systems, the requirements referred to in Paragraph 15 of this Regulations shall be taken into account and the following shall be additionally provided:

24.1. the password for each system user is mandatory changed not later than after 90 days, however the password is prohibited to be independently changed more than twice within 24 hours;

24.2. a password for the system user is selected by avoiding its matching with the previous five passwords of the system user;

24.3. the account (except for the account of the system administrator) is immediately blocked if incorrect password of the account of the system user is entered five consecutive times;

24.4. the account of the system administrator, using equipment located outside the premises of the authority and the equipment other than in the possession of the authority allows accessing the system only by using multi-factor authentication;

24.5. only the authorised persons of the authority may physically access the equipment ensuring the operation of the system;

24.6. the creation and storage of system (both service and operating system) trails (covering the system audit trail data – authentication data and network flow audit data, Domain Name System (DNS) server trails, Intrusion Detection Systems (IDS) trails, operating system authentication trails) are ensured for at least 18 months after making an entry by storing the system trails or their copies separately from the system;

24.7. system trails are created by ensuring that the time indicated therein matches the coordinated universal time (UTC) of the actual event with a precision of one second;

24.8. a systematic supervision and analysis of the content of the system trail is ensured to establish any incidents;

24.9. error notifications displayed to the system users contains only the minimum necessary information for the system user to resolve the error independently or by assistance of the system support staff;

24.10. the flow between the system and its users, and also between the system and other systems is controlled, for example, by using the firewall;

24.11. network services not used for ensuring the system operation are disconnected;

24.12. making a threat to the integrity of data stored in the system is not allowed by carrying out development and testing of the system;

24.13. placement of the system in the resources ensured by the provider of the outsourced services is allowed only if the service provider is a legal person registered in the European Union Member State or the European Economic Area State, and the information stored in the system is located only on the territory of the European Union Member State or the European Economic Area State.

[*15 January 2019*]

25. The internal security regulations of the system shall determine:

25.1. the procedures for the creation, supplementing, changing, processing, transmission, storage, updating and destruction of the information resources of the system;

25.2. the procedures for the use of the information and technical resources of the system and control thereof;

25.3. the procedures for the ensuring access to the information and technical resources of the system;

25.4. the procedures for the creation and storage of the reserve copies of the information resources of the system, and also the procedures for verifying a possibility of restoring the information resources of the system by using the reserve copies of the information resources of the system;

25.5. the procedures for the using, moving, storage and destruction of the data carriers;

25.6. the procedures for the using and storage of the information or data necessary to access the information or technical resources of the system;

25.7. the requirements for the protection of the information resources of the system carried out using the software tools (for example, recognition of the system user and conformity verification of his or her authority with the respective activities in the system, by protecting the information resources of the system from direct or indirect incidental damaging or destruction);

25.8. requirements for the protection of the technical resources of the system against the threats to security of the system caused by physical actions (for example, fire, flood, reduction of power or overvoltage in the power supply network, theft of the technical resources of the system, humidity or temperature not conforming to the conditions of use);

25.9. the procedures for the monitoring the features of approaching of the security threat of the system;

25.10. the procedure for the detecting and managing the security incidents of the system;

25.11. the procedures for the operating the system if the information or technical resources of the system are not available in full scope;

25.12. the procedures for the changing the technical resources;

25.13. the procedures for the training and testing knowledge of the staff of the authority in the field of system security;

25.14. the procedures for assessing the impact of the system upgrades to be introduced on the system security;

25.15. the procedures for the creation, storage, processing, and deletion of system trail files.

[*15 January 2019*]

26. The provisions for use of the system shall include:

26.1. rights, obligations, restrictions and responsibility of the system users;

26.2. the procedures for the registration of the system users and cancellation thereof;

26.3. the procedures for the use of the system;

26.4. the procedures for support of the system users.

27. The security risk management plan of the system shall include:

27.1. a description of the methodology of the risk analysis to be carried out;

27.2. security risk analysis of the system;

27.3. the measures for mitigation of the security risk of the system, time periods for performance thereof, financing and a list of the persons responsible for the performance.

28. Acceptable level of the security risk of the system shall be ensured during implementation of the security risk management plan of the system.

29. The security risk management plan of the system shall be developed and updated based on the security risk analysis of the system.

30. The security risk analysis of the system shall include:

30.1. a list of threats to security of the system, an assessment of their likelihood and a list of signs for their approaching;

30.2. an assessment of the potential damages or harm to the authority, data subjects of the system and users of the system in case of the security incident of the system;

30.3. security risk assessment of the system;

30.4. a list of the measures for mitigation of the security risk of the system and tools used therein;

30.5. rationality assessment of the measures performed for mitigation of the security risk of the system.

31. [15 January 2019]

32. The authority shall ensure that the tools used in the measures for mitigation of the security risk of the system would be commensurate to the potential losses or harm caused to the authority, data subjects of the system and users of the system as a result of the security incident of the system.

33. The restoration plan of the system operation shall include:

33.1. the restoration measures for the information and technical resources of the system to be carried out after a security incident of the system;

33.2. a description of the procedures of measures for the restoration of the system operation;

33.3. the procedures for the informing the responsible persons involved in the restoration measures of the system operation and instructions for activities;

33.4. a plan of training, lessons and preparedness testing of the responsible persons.

34. The authority shall ensure the testing of the security of system referred to in Paragraph 12 of this Regulation for the increased security systems available by using the public data transmission network at least once within two years by ordering external audit of the security documentation and performance of the intrusion tests.

[*19 December 2017*]

35. By ordering the external security audit for the security system, the authority shall stipulate that the legal person performing an audit is registered in a Member State to the NATO, the European Union or the European Economic Area, its employees involved in performance of the audit are citizens of the states to the NATO, the European Union, the European Economic Area or non-citizens of the Republic of Latvia, and the legal person processes the information obtained during the audit only in the territory of the states to the NATO, the European Union or the European Economic Area.

36. The outsourcing contract for the maintenance of increased security systems may only be concluded with:

36.1. a legal person:

36.1.1. registered in a Member State to the NATO, European Union, or European Economic Area;

36.1.2. the beneficial owner of which is a citizen of a NATO, European Union, or European Economic Area country or a non-citizen of the Republic of Latvia;

36.1.3. the manufacturer of the software or equipment used to provide the service is a legal person registered in a Member State to the NATO, European Union, or European Economic Area or a natural person who is a national of the Republic of Latvia or a citizen of a NATO, European Union, or European Economic Area country;

36.2. a natural person who is a citizen of a NATO, European Union, or European Economic Area country or a non-citizen of the Republic of Latvia.

[*11 August 2020 / See Paragraph 44*]

36.1 The contract for the purchase of services, software, or equipment for increased security systems may be concluded with:

36.11. a legal person:

36.11.1. registered in a Member State to the NATO, European Union, or European Economic Area;

36.11.2. the beneficial owner of which is a citizen of a NATO, European Union, or European Economic Area country or a non-citizen of the Republic of Latvia;

36.11.3. the manufacturer of the software or equipment used to provide the service is a legal person registered in a Member State to the NATO, European Union, or European Economic Area or a natural person who is a national of the Republic of Latvia or a citizen of a NATO, European Union, or European Economic Area country;

36.12. a natural person who is a national of the Republic of Latvia, a citizen of a NATO, European Union, or European Economic Area country.

[*11 August 2020 / See Paragraph 44*]

36.2 Legal persons governed by private law that have been recognised as the operators of essential services or the systems in the ownership or possession whereof have been recognised as the information systems of the critical infrastructure, within a period of six months from the day on which the decision to grant the status of the operator of essential services or on recognition as the critical infrastructure is taken, shall ensure that the respective systems conform to the requirements laid down in this Regulation.

[*15 January 2019*]

36.3 Paragraphs 36 and 36.1 of this Regulation shall not apply if an opinion has been received from the competent State security institution that the contract may be concluded.

[*11 August 2020*]

36.4 The authority shall specify in the contracts referred to in Paragraphs 36 and 36.1 of this Regulation the obligation of the supplier to notify immediately of a change of the beneficial owner during the term of the contract. The contract shall be terminated if the restriction on the beneficial owner specified in Paragraphs 36 and 36.1 of this Regulation has occurred and the competent State security institution has not agreed to the continuation of the contract.

[*11 August 2020 / See Paragraph 46*]

**IV. Closing Provisions**

37. Cabinet Regulation No. 765 of 11 October 2005, General Security Requirements of State Information Systems (*Latvijas Vēstnesis*, 2005, No. 164, 2008, No. 195, 2009, No. 85, 2010, No. 150, 2011, No. 19) is repealed.

38. The State and local government authorities shall approve the documents referred to in Paragraph 8 of this Regulation by 1 January 2017. The documents drafted prior to coming into force of this Regulation in respect of the State information systems shall remain in effect insofar as they do not contradict with this Regulation.

[*15 January 2019*]

39. In respect of basic security systems, which have been transferred for use to the institutions by 1 January 2017, Paragraph 15 of this Regulation shall be applied from 1 January 2021.

40. In respect of the increased security systems, which have been transferred for use to the institutions by 1 January 2017, Paragraphs 15 and 24 of this Regulation shall be applied from 1 January 2018.

41. If by the day of application of Paragraphs 15 and 24 accordingly referred to in Paragraphs 38 and 39 of this Regulation the system does not comply with the minimum security requirements, its use shall be terminated within a year after the date of application referred to in the relevant Paragraph, ensuring that the functions of the system, where necessary, are taken over by the system of the same or other authority.

42. The authority shall, from 1 January 2019, ensure the external security documentation audit and intrusion tests for the increased security systems referred to in Paragraph 34 of this Regulation that are available by using a public data transmission network.

[*19 December 2017*]

43. The requirements laid down in this Regulations shall be applied to legal persons governed by private law that are the owners or lawful possessors of the critical infrastructure of information technologies, the operators of essential services and digital service providers from 1 May 2019.

[*15 January 2019*]

44. The requirement of the beneficial owner referred to in Paragraphs 36 and 36.1 of this Regulation shall apply to the procurement procedures which have been announced after 1 September 2020.

[*11 August 2020*]

45. Sub-paragraphs 15.15 and 15.16 of this Regulation shall come into force on 1 January 2021.

[*11 August 2020*]

46. Sub-paragraphs 20.3.5 and 20.3.6 and Paragraph 36.4 of this Regulation shall apply to the contracts concluded after 31 August 2020.

[*11 August 2020*]

**Informative Reference to the European Union Directive**

[*15 January 2019*]

This Regulation contains legal norms arising from Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Acting for the Prime Minister – Minister for Transport Anrijs Matīss

Minister for Defence Raimonds Bergmanis