Printed from the Register of Legal Acts.

Risi:	Resolution	Date of adoption:	2024-11-06	Valid Aggregate Resolution:	Nera
Registration data.	No. 2024-19589	No. issued by the institution:	945	List of cumulative orders by dateq:	Nera
Valid	Effective 12-11-2024	Adopted:	Government of the Republic of Lithuania	Draft amendments:	Nera
Ex post evaluation:	None	Published:	TAR, 11-11-2024, No. 19589	Eurovoc terms:	Yra
				Relationship to EU legislation:	there is no

GOVERNMENT OF THE REPUBLIC OF LITHUANIA

RULING
THE GOVERNMENT OF THE REPUBLIC OF LITHUANIA ON **13 AUGUST 2018 818 of the Government of the Republic of Lithuania of August 18, 2018 on 'AMENDMENT TO THE Cybersecurity Law of the Republic of Lithuania'**

6 November 2024 No 945 Vilnius

The Government of the Republic of Lithuania hereby:

1. To amend the Resolution of the Government of the Republic of Lithuania No 818 of 13 August 2018 "On the Implementation of the Law on Cyber Security of the Republic of Lithuania" and to reword it:

"THE GOVERNMENT OF THE REPUBLIC OF LITHUANIA

RESOLUTION
ON THE IMPLEMENTATION OF THE CYBERSECURITY LAW OF THE REPUBLIC OF LITHUANIA

Pursuant to Article 7(2)(3), Article 11(6), Article 14(1) of the Law on Cyber Security of the Republic of Lithuania 1 punktu ir 2 dalimi, 28 straipsnio 6 dalimi, 30 straipsnio 1 dalimi, 37 straipsnio 1 dalimi, 2 dalies 3 punktu, 4, 6, 8 ir 9 dalimis ir įgyvendindama 2022 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on a measure to ensure a high common level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148, the Government of the Republic of Lithuania shall:

1. To approve the accompanying documents:

1.1. National Cyber incident management plan;

1.2. Methodology for the identification of cybersecurity entities according to specific criteria;

1.3. Description of cyber security requirements;

1.4. A description of the procedures for applying enforcement measures to cybersecurity entities;

1.5. The list of users of the secure national data transmission network;

1.6. the description of the criteria for determining the amount of remuneration for the use of additional e1ectronic communications and cyber security services provided by the Secure State Data Transmission Network and the description of the procedure for calculating the remuneration.

2. Jgalifice:

2.1. Approved by the Minister for National Defence:

2.1.1. Conditions and rules for the provision of electronic communications and cybersecurity services over the secure national data transmission network;

2.1.2. the conditions, plan and terms of connection and disconnection of users of the Secure State Data Communications Network to and from the Secure State Data Communications Network, the list of cases of connection to the public electronic communications network outside the Secure State Data Communications Network, and the description of procedures;

2.2. the Ministry of National Defence of the Republic of Lithuania to assess whether the amounts of remuneration for the use of additional electronic communications and cybersecurity services provided by the Secure State Data Communications Network are determined in accordance with the criteria for determining the amount of remuneration for the use of additional electronic communications and cybersecurity services provided by the Secure State Data Communications Network and to provide an opinion to the manager of the Secure State Data Communications Network;

2.3. the National Cyber Security Centre under the Ministry of National Defence to submit recommendations to the Minister of National Defence on the classification of state and municipal institutions and establishments, state-owned enterprises and public bodies (hereinafter referred to as 'institutions') as vital institutions for national security, defence or life-supporting state functions.

3. Instruct cybersecurity entities to adapt their cybersecurity incident and cyber incident management networks and information systems within 12 months of their registration in the Register of Cybersecurity Entities, so that cyber incidents are automatically registered in the National Cybersecurity Incident Management Platform, which is hosted in the Cybersecurity Information System. For the cybersecurity entity

if, due to objective reasons, it is not able to comply with the requirement set out in this point and upon submission of a reasoned request, the National Cyber Security Centre under the Ministry of National Defence shall have the right to extend the term once, but not more than 12 months."

2. Annulled:

2.1. Resolution of the Government of the Republic of Lithuania No 716 of 24 July 2013 "On the approval of the description of the Community electronic information security requirements and the description of the guidelines for the content of security documents", as amended and supplemented;

2.2. Resolution No 27 of 3 January 2018 of the Council of Ministers of the Republic of Lithuania 'On the implementation of the Law of the Republic of Lithuania on the Management of State Information Resources in the field of the Secure State Data Transmission Network', as amended and supplemented.

The Prime Minister The Ingrida Šimonyiê

Minister for National Laurynas Kasčiiinas

Defence

APPROVED
of the Government of the Republic of Lithuania
by Resolution No. 818 of the Government of the
Republic of Lithuania of 13 August 2018
wording of Decree No 945 of 6 November
2024)

NATIONAL CYBER INCIDENT MANAGEMENT PLAN

CHAPTER I GENERAL PROVISIONS

1. The National Cyber Incident Management Plan (hereinafter referred to as "the Plan") establishes the management, assessment and reporting o f cyber incidents.

2. The terms used in the Plan shall be understood as defined in the Law on Electronic Communications of the Republic of Lithuania, the Law on Information Society Services of the Republic of Lithuania, the Law on Cyber Security of the Republic of Lithuania, the Law on Crisis Management and Civil Protection of the Republic of Lithuania, the Law on State and Service Secrets of the Republic of Lithuania, the Law on Management of State Information Resources of the Republic of Lithuania, the Law on Information Security of the Republic of Lithuania, the Law on the Information Security of the Republic of Lithuania, the Law on the State Information Resources Management of the Republic of Lithuania, the Law on the Information Security of the Republic of Lithuania, the Law on the State and Service Secrets of the Republic of Lithuania, and the Law on the State Information Resources Management of the Republic of Lithuania. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Cyber Security Agency) and the certification of information and communication technologies for cyber security and repealing Regulation (EU) No 526/2013.

CHAPTER 11 CYBER INCIDENT MANAGEMENT

3. The organisation of the management of cyber incidentsq at the level of the cybersecurity entity is managed by the cybersecurity entity. The organisation of cyber incident management shall be ensured by performing the functions provided for in points 24 and 25 of the description of cyber security requirements approved by this Government Resolution and by appointing persons performing these functions to the head of the cyber security entity or his/her delegate (hereinafter referred to as the 'Security Operations Centre'). The cybersecurity entity shall ensure that the functions of the Security Operations Centre are no longer delegated to an employee of the cybersecurity entity or of the service provider who is responsible for the proper functioning of that cybersecurity entity's network and/or information system.

4. The cybersecurity entity shall organise the management of cyber incidents in accordance with a cyber incident management plan approved by the cybersecurity entity. This plan must include the actors, stages, factors, timelines and deliverables set out in the Typical Cyber Incident Management Process Flowchart (Annex 1 to the Piano) and the Typical Cyber Incident Management Process Outline (Annex 2 to the Piano).

5. A cyber incident is considered contained when the services provided by the cyber security entities' networks and information systems are restored.

6. At the national level, the management of cyber incidents shall be carried out by the National Cyber Security Centre under the Ministry of National Defence (hereinafter referred to as the NCSC) in accordance with the National Cyber Incident Management Process Scheme (Annex 3 to the Plan) and the description (Annex 4 to the Piano).

7. The NSCC, when deciding on the allocation of resources for the management of a major cyber incident upon the request of a cybersecurity entity, shall take its decision after assessing the likelihood of the major cyber incident becoming an emergency. Priority shall be given to cyber incidents whose consequences most closely meet or exceed the criteria for an emergency as defined by the Government.

8. In the event of a major cyber incident that meets the criteria for an emergency incident, or is threatened to do so, the NCSC shall inform the National Crisis Management Centre (NCMC) of the Cabinet Office.

CHAPTER III
CYBER INCIDENT IMPACT ASSESSMENT AND CYBER INCIDENT REPORTING

9. Unless further specified by the implementing legislation of the European Commission, a major cyber incident within the meaning of Article 18(2) of the Law on Cyber Security shall be deemed to have occurred when:

9.1. the cybersecurity entity is experiencing or is likely to experience a major service disruptionq and the cyber incident meets at least one of the iiq criteriaq:

9.1.1. services are disrupted throughout the territory of Lithuania and/or in at least one country of the European Union or NATO;

9.1.2. the network and information system is disrupted for 2 hours or more;

9.1.3. the number of jobs affected is equal to or greater than 1 000 or 25 per cent (w h i c h e v e r is the lower);

9.1.4. 1 000 or 25 per cent (whichever is the smaller) of the service recipient's personal data or other data of the recipient held by the cybersecurity entity are affected;

9.1.5. the cybersecurity entity is no longer able to ensure the fulfilment of the requirements imposed on its activities by law;

9.1.6. loss or disclosure of trade secrets or classified information;

9.1.7. more than one analogous cyber incident occurs within a period of 6 months, the root cause of which is the same and the amount of the financial loss reaches the values provided for in sub-paragraph 9.2;

9.2. the cybersecurity entity has suffered or is likely to suffer a substantial financial loss equal to or greater than EUR 500 000 or 5 per cent of the cybersecurity entity's last financial year's turnover (whichever is the lesser);

9.3. the cyber incident has affected or is likely to affect other natural or legal persons, causing significant material or non-material damage meeting at least one of the following criteria:

9.3.1. the amount of the potential pecuniary damage is equal to or more than 400 basic social security benefits;

9.3.2. the amount of the potential non-pecuniary damage is equal to or more than EUR 10 000;

9.3.3. the health of at least one person is affected or at least one person is killed.

10. The Security Operations Centre of the cybersecurity entity shall inform the NCSC of cyber incidents by registering them in the subsystem of the Cybersecurity Information System - the National Cyber Incident Management Platform (hereinafter referred to as the Platform).

11. The Security Operations Centre of a cybersecurity entity which, due to a cyber incident, is not in a position to notify cyber incidents in an automated manner via the Platform, shall inform the NCSC by filling in a form on the Platform, on the NCSC's website, at the email address or by telephone indicated by the NCSC.

12. The Security Operations Centre of the cybersecurity entity shall inform the NCSC of a major cyber incident within the deadlines set out in Article 18(4) of the Law on Cybersecurity, by providing the information referred to in the same paragraph. The Security Operations Centre of the cybersecurity entity shall have the right to provide other information not specified in Article 18(4) of the Cybersecurity Law but relevant for the management or investigation of a major cyber incident.

13. The Security Operation Centre of the cybersecurity entity shall inform the NCSC of other cyber incidents that do not comply with the provisions of Article 18(2) of the Law on Cybersecurity and Clause 9 of the Plan (hereafter referred to as "minor cyber incident") by submitting:

13.1. immediately, but no later than 72 hours from the moment of becoming aware of the cyber incident, by submitting a notification of a minor cyber incident, including the information referred to in Article 18(4)(2) of the Law on Cybersecurity;

13.2. within one month of the date of registration of the cyber incident report, a final report on the minor cyber incident, containing the information referred to in Article 18(4)(4) of the Law on Cybersecurity. A final report on a minor cyber incident shall not be submitted if the cyber incident report contains all the information in the final report.

14. The Security Operations Centre of a cybersecurity entity shall, when providing the NCSC with the information referred to in Article 18(2) of the Law on Cybersecurity on the initial assessment of a cyber incident, state:

14.1. what service disruption the cybersecurity entity has experienced or may experience - the scope of the service and the disruption;

14.2. the financial loss suffered or likely to be suffered by the cybersecurity entity, indicating the amount of the loss;

14.3. whether the cyber incident has affected or is likely to affect other persons, causing material or non-material damage - if so, the persons and the amount of damage;

14.4. evidence of unlawful or malicious acts (if any);

14.5. whether the incident was contained;

14.6. other relevant information (e.g. the location of the cyber-victim, the exact time of detection).

15. If the cyber incident continues for more than one month, the information referred to in Article 18(4)(2) of the Law on Cyber Security shall be updated on a monthly basis by the cybersecurity entities.

16. At the request of the NCSC, a cybersecurity entity shall submit interim reports on major cyber incidents within the timeframes specified by the NCSC. The NCSC shall have the right to request the submission of other data necessary and relevant for the management of a major cyber incident.

17. Persons who are not obliged to report cyber incidents to the NCSC shall voluntarily report cyber incidents, cyber threats, near misses and/or cyber incident management measures to the NCSC:

17.1. the Security Operations Centre of the cybersecurity entity, in the same way as for cyber incidents;

17.2. persons who are not cybersecurity subjects - according to the guidelines published on the NCSC website.

18. When providing the information referred to in Article 18(4)(4)(b) of the Cybersecurity Law, one of the listed cyber threats and the root cause of the incident shall be selected:

18.1. dissemination of unsolicited messages and/or abusive *content* (*abusive content, spam)* and/or disruption of the network information system;

18.2. *malicious software/code:* software, or any part thereof, that facilitates unauthorised access to, take control of, disrupt or alter the operation of a network or information system, destroy, corrupt, erase or alter digital data, deny or restrict access to it, and misappropriate or otherwise exploit non-public digital data of p e r s o n s not having the right, and which is identified as:

18.2.1. *advanced persistent threat* (*API)* software*;*

18.2.2. network and information system data encryption and destruction (*w'iper)* or ransomware (w*'iper*).
ransomware,'

18.2.3. parts of the network and information system that are under the active control of the ¡sibrovê1ii¡;

18.2.4. distribution of malicious software;

18.3. *in%rmation gathering:* intelligence or other suspicious activities, manipulation of the user's emotions, psychology, inattention, exploiting technological ignorance (*social engineering)* to monitor and gather information, to discover weaknesses, to perform threatening actions, to deceive the user into disclosing information (*phishing)* or to perform insane actions. Social engineering techniques are used to lure network and information system logins and/or other sensitive information;

18.4. *Intrusion attempts*. Attempts to hack or disrupt the operation of a network and information system by exploiting known vulnerabilities*, login attempts,* new *attack signatures, which* may be categorised as follows.

18.4.1. Exploitation of one or more unknown vulnerabilities (*zero day);*

18.4.2. network and information system reconnaissance or other malicious activity (port scanning, password selection, m a l w a r e distribution, etc.);

18.4.3. Exploitation of known and publicly disclosed vulnerabilities;

18.5. irtinsions. Successful hacking and/or unauthorised use of a network and information system, application software or service (*privileged account compromise, unprivileged account compromise, application compromise), which is* categorised as follows:

18.5.1. access to the network and information system or its security measures, misappropriation of information, destruction of information, damage to the network and information system or to part of the network and information system, which disrupts the uninterrupted provision of the services provided by the network and the information system, and which may affect the reliability of the information processed and the services provided, and which may affect the content of, and undermine the confidence of, the users of the network and the information system in them;

18.5.2. unauthorised access to the network and information system, application software or service;

18.6. Disruption of service, availability*:* actions that disrupt the operation of a network and information system, disrupt the services provided (*DoS, DDo fi),* damage to a network and information system or part of a network and information system, disrupting the operation of the timid and information system and/or the services it provides, which are categorised as:

18.6.1. interruption of the service provided or exceeding the maximum permissible time of inactivity of the service;

18.6.2. disruption of the uninterrupted provision of a service, which may affect the availability of the information and/or services processed;

18.7. *supply chain attack:* exploiting the infrastructure of a third party providing services to a network and information system operator and/or manager in order to obtain or affect services on the infrastructure of the recipient network and information system;

18.8. *information content s e c u r i t y* breaches*:* unauthorised access to, or unauthorised modification of, information which may h a v e an impact on the operation of the network and information system and/or the services provided;

18.9. unauthorised *use* of *resources,* unauthorised use of s o f t w a r e or *copyright*, identity fraud, fraud and other similar incidents;

18.10. other threats or causes.

19. Upon registration of an incident, information about a possible criminal offence or violation of the protection of personal data using the Platform shall be submitted to the Lithuanian Police and/or the State Data Protection Inspectorate as appropriate. Upon receipt of information on a cyber incident, the NCSC and other authorities referred to in paragraph 1 shall take decisions on the initiation of an investigation within their competence. Data on cyber incidents necessary for institutional investigations, except for pre-trial investigation data, shall be submitted and processed on the Platform.

20. The NCSC, the Lithuanian Police and the State Security Inspectorate, upon receiving or identifying cyber incidents, shall immediately, but no later than within 24 hours from the moment of receiving or identifying cyber incidents, register the cyber incidents in the Platform, providing all the available information, and shall inform the Cyber Security Entity's Security Operations Centre thereof. The following shall be notified to the institution

Cyber incidents are reported to the Security Operations Centres of the cybersecurity entities via the Platform. The Security Operations Centre of the cybersecurity entity must provide the information referred to in Article 18(4)(1) or (2) of the Cybersecurity Act within the time limits set out in the Plan.

21. The NCSC, after having evaluated the information on cyber incidents on the Platform and having determined that a minor cyber incident should be classified as a major cyber incident, shall classify the cyber incident on the Platform as a major cyber incident and shall inform the cybersecurity entity of this fact immediately, but at the latest within 24 hours of the discovery of the incident referred to in this paragraph.

22. Where a major cyber incident involves two or more Member States, the NCSC shall inform the other affected Member States and the European Union Network and Information Security Agency (hereinafter referred to as 'ENISA') of the major cyber incident no later than 24 hours from the time of becoming aware of the incident.

23. The NCSC shall submit a summary report to ENISA every 3 months, including personalised and aggregated data on cyber incidents, cyber threats and near misses.

24. Information on major cyber incidents, cyber incidents, cyber threats and near misses reported by cybersecurity entities that have been recognised as entities of particular importance in accordance with the Law on Crisis Management and Civil Protection shall be reported by the NCSC to the NCCC no later than 24 hours from the time of becoming aware of them. The NCSC shall notify the NCCC of registered major cyber incidents in cybersecurity entities which have been recognised as entities of critical importance in accordance with the Law on Crisis Management and Civil Protection without delay, but not later than within 1 hour from the time of registering the cyber incident. Summary information on cyber incidents, cyber threats and near misses in the cybersecurity entities referred to in this point shall be provided by the NCSC to the NCCC every 3 months.

AFFIRMED
The Government of the Republic of Lithuania
by Resolution No. 818 of the Government of the
Republic of Lithuania of 13 August 2018
(Government of the Republic of Lithuania
wording of Decree No 945 of 6 November 2024)

METHODOLOGY FOR THE IDENTIFICATION OF CYBERSECURITY ACTORS ACCORDING TO SPECIFIC CRITERIA

CHAPTER I GENERAL PROVISIONS

1. The Methodology for the Identification of Cyber Security Entities according to Special Criteria (hereinafter referred to as the Methodology) establishes the procedure for the identification of cyber security entities according to the special criteria for the identification of cyber security entities (hereinafter referred to as the Special Criteria), as set out in Article 11(5) of the Law on Cyber Security of the Republic of Lithuania.

2. The Annex to the Methodology sets out the values of the special criteria, whereby if at least one of them is met, the entity shall be classified as an essential cybersecurity entity (hereinafter referred to as "essential entity") or an important cybersecurity entity (hereinafter referred to as "important entity").

3. The authorities responsible for identification, as well as the ministries responsible for shaping
(hereinafter referred to as "Responsible Authority") may identify the entities falling within the scope of the sector, taking into account the specific criteria set out in| .

4. The Responsible Authorities must designate the persons responsible for the identification of the entity and provide the contact details of the person responsible for the designation to the Cybersecurity Information System (hereinafter referred to as 'CISA') Data Manager in accordance with the procedure laid down in the CISA Regulations.

5. The identification of cybersecurity entities in accordance with this Methodology shall be carried out in the CISA.

6. The terms used in the Methodology shall be understood as defined in the Law on Cyber Security, the Law on Crisis Management and Civil Protection of the Republic of Lithuania, the Law on Public Administration of the Republic of Lithuania.

CHAPTER II
identification of cybersecurity entities

7. The CISA Data Processor shall draw up a preliminary list of cyber security entities to be identified according to the specific criteria, which shall include the data on cyber security entities referred to in Article 13(3) of the Law on Cyber Security, which are known to the CISA Data Processor, and shall inform the Responsible Authorities of the establishment of the list.

8. The Responsible Authority shall evaluate the preliminary list of cybersecurity entities within no later than ninety working days from the date of receipt of the notification referred to in point 7 of this Methodology, if it finds a deficiency, and shall amend or supplement the list with new cybersecurity entities which meet the specific identification criteria.

9. The responsible authority, having assessed the preliminary list of cybersecurity entities, shall inform the entity of its inclusion in the preliminary list of cybersecurity entities and shall request the entity to confirm the correctness of the data submitted or to improve the data submitted in accordance with the specific values of the criteria set out in the Annex to the Methodology, within ten working days of the receipt of the notification. After the expiry of the ten working days and without a reply from the subject, the subject shall be deemed to have accepted that the data submitted are correct. The subject has the right to request an extension of the deadline for submitting the reply, which the Responsible Authority may extend once for a maximum of ten working days. The Responsible Authority shall have the right to request additional information from the entity that is necessary to update the preliminary list of cybersecurity entities.

10. The responsible authority shall, at the latest within ten working days of receipt of the reply referred to in point 9 of the Methodology, if a reply has been submitted, evaluate the entity's reply and, if necessary, provide the entity with comments and observations, and shall ask the entity to confirm the correctness of the data submitted or to revise the data submitted, within ten working days of the receipt of the communication.

11. If the Responsible Authority which has started the evaluation of the entity considers that the identification of the entity falls within the competence of another Responsible Authority, it shall contact the CIS Data Manager and the latter shall decide which Responsible Authority is to evaluate the entity at the latest within five working days from the date of receipt of the contact.

12. The Responsible Authority shall, after completing the evaluation of the preliminary list of cybersecurity entities or part thereof, which may not take longer than three
months from the date of receipt of the information referred to in point 7 of the Regulation, it shall notify the KSIS data manager thereof.

13. The CISA Data Processor shall, upon receipt of the information from the Responsible Authority on the completion of the assessment of the preliminary list of cybersecurity entities or a part thereof, add the entities of the preliminary list of cybersecurity entities to the list of cybersecurity entities by registering them in the CISA.

14. The CISA Data Processor shall update the list of preliminaitţ cybersecurity entities at least once a year in case of changes,
notify the Responsible Authority. The QISM and the Responsible Authority shall continue to carry out the actions set out in points 8 to 13 of this Methodology.

CHAPTER III FINAL PROVISIONS

15. The data of an entity which fulfils the specific criteria and which has independently submitted data to the QSIS Data Manager in accordance with the procedure laid down in the QSIS Regulations shall be evaluated in accordance with the procedure laid down in Chapter II of this Methodology.

16. The responsible authority, upon receiving a notification from a cybersecurity entity or upon independently identifying that a cybersecurity entity does not meet the identification criteria of the speeialiitjq, shall notify the CISA Data Processor and update the data on the cybersecurity entity in the CISA. The data received shall be evaluated in accordance with the procedures laid down in the CIS Regulations.

17. The CISA Data Processor shall update the data on entities operating in the sectors and subsectors listed in Annexes 1 and 2 to the Law on Cyber Security at least once a year and shall inform the Responsible Authority of new data.

18. The Responsible Authority shall, at least once a year, update in the CISA, in the areas of governance entrusted to the Minister, the data on the entities operating in other sectors and sub-sectors which are not listed in Annexes 1 and 2 of the Law on Cyber Security and which potentially meet the specific criteria for identification of a cyber security entity.

Methodologies for the identification of
cybersecurity entities according to the
specific criteria
Annex

VALUES FOR THE IDENTIFICATION OF A CYBERSECURITY ENTITY ACCORDING TO THE SPECIFIC CRITERIA

Eü N	Specific identification criterion
1.	The entity is the sole provider of a service which is necessary to ensure the performance of a critical public or economic activity in Lithuania
2.	The disruption of a service provided by the entity may have a major impact on public safety, public security or public health
3.	The disruption of a service provided by the entity is likely to pose a significant systemic risk in sectors where such disruption is likely to have a cross-border impact
4.	The entity is of particular interest because of its specific relevance to a particular sector or service area or other interdependencies

Eil. No.	Specific identification criterion
5.	The entity provides services and/or carries out activities in the sector of public administration referred to in Annex 1 of the Law on Cyber Security, which are subject to the following to the public and is considered as a territorial public administration entity or a regional administration entity or a municipal administration entity under the Law
6.	Disruption of a service provided by the entity may have a significant impact on the essential service and/or activities provided by the entity
7.	The entity is a provider of a service that is necessary for the performance of vital State functions and State mobilisation tasks
8.	The entity carries out critical research and expertise in the sector of scientific research specified in Annex 2 to the Cyber Security Act

APPROVED
by the Government of the Republic of Lithuania
by Resolution No. 818 of the Government of the
Republic of Lithuania of 13 August 2018
(Government of the Republic of Lithuania
Resolution No. 945 of the Republic of Lithuania of
6 November 2024)

DESCRIPTION OF CYBER SECURITY REQUIREMENTS

CHAPTER I
GENERAL PROVISIONS

1. The Cybersecurity Requirements Schedule (hereinafter referred to as 'the Schedule') sets out the cybersecurity requirements for cybersecurity entities.

2. The terms used in the Description are defined in the Law on Electronic Communications of the Republic of Lithuania, the Law on Information Society Services of the Republic of Lithuania, the Law on Cyber Security of the Republic of Lithuania, the Law on Management of State Information Resources of the Republic of Lithuania, the Law on Public Procurement of the Republic of Lithuania, and in the Lithuanian Standard LST EN ISO/IEC 27002.

3. The cybersecurity entity, when implementing the requirements of the Description concerning the approval of documents, shall have the right to choose to place the provisions implementing the specified requirements in a single document or to set them out in separate documents.

CHAPTER II
CYBERSECURITY REQUIREMENTS

SECTION 1
SECURITY POLICY FOR NETWORKS AND INFORMATION SYSTEMS

4. The head of the cybersecurity entity or his/her delegate must approve a cybersecurity policy document for the network and information system, which must state:

4.1. the objectives of the cybersecurity activities, formulated in accordance with the cybersecurity principles set out in the Cybersecurity Law;

4.2. a list of the legal acts governing cybersecurity which shall be followed;

4.3. other cybersecurity policy documents that guide the implementation of the network and information system security policy;

4.4. the obligations of the cybersecurity policy to be respected by employees and third parties;

4.5. the obligation to review and update the cybersecurity policy documents on a regular basis, at least annually or as circumstances change.

5. Cybersecurity entities shall submit and/or update the validation data of the cybersecurity policy document (-q), indicating the name of the document, the date of validation and the registration number, to the National Cyber Security Centre under the M i n i s t r y of National Defence (hereinafter referred to as the NSCC) through the Cybersecurity Information System (hereinafter referred to as the CIS) no later than within 5 working days from the day of the validation and/or amendment of the document (-q).

6. The NCSC, when conducting an inspection of a cybersecurity entity, shall have the right to request the submission of copies of the document referred to in point 3 of the Description to the KSIS no later than within 5 working days from the date of receipt of the request by the NCSC.

SECTION 2 CYBERSECURITY RISK ANALYSIS

7. The head of the cybersecurity entity or his/her ţauthorised person shall establish a procedure for the risk assessment and management of the cybersecurity entity's network and information system, including:

7.1. the appointment of a person or person with responsibility for risk assessment, oversight and continuous improvement of the risk assessment process;

7.2. the assessment and management process;

7.3. a risk level acceptable to the cybersecurity entity;

7.4. requirements for the frequency of the risk assessment.

8. The risk assessment and management process shall include at least the following elements:

8.1. Identification and classification of networks and information systems;

8.2. risk analysis, including analysis and assessment of threats and gaps, potential impacts, risk calculation;

8.3. selection of risk management measures.

9. The risk assessment shall be carried out at least once a year, in the event of a major organisational or other significant change in the cybersecurity entity, as well as in the event of a major cyber incident.

10. Following the risk assessment, cybersecurity entities shall prepare a risk assessment report and, if the risk assessment identifies a vulnerability, a risk management plan, which shall be approved by the head of the cybersecurity entity or his/her delegate.

11. The risk assessment report shall include at least the identification of the assets in the tînklq and înformaciniq system, the impact assessment, the information from the threat and gap assessment and the results of the risk calculation according to the criteria established by the cybersecurity entity, as well as the management of the risk.

12. The risk management plan shall include at least the identification of measures to manage unacceptable risks and the resources required, the persons responsible for t h e implementation o f the measures, and the timeframe for the implementation of the measures.

13. The cybersecurity entity shall provide the validation of the risk assessment report and the risk management plan, indicating the date of validation and the registration number, and the aggregated results of the risk assessment: threats identified, likelihood and impact on operations, risk levels and management measures, to the CISA no later than 5 working days after the validation of the risk assessment documents.

14. Risk assessment reports and risk management plans approved by the head of the cybersecurity entity or his/her delegate shall be kept f o r at least 3 years.

15. The NCSC shall have the right to require the cyber security entity to provide a copy of the risk assessment report and a copy of the risk management plan when conducting an inspection of the cyber security entity. The cybersecurity entity shall submit these documents to the CISA no later t h a n within 5 working days from the date of receipt of the request by the NCSC.

SECTION THREE
DUTIES OF THE PERSON RESPONSIBLE FOR CYBERSECURITY AND THE HEAD OF THE CYBERSECURITY ENTITY OR H I S / H E R DELEGATE

16. The head of the cybersecurity entity or his/her delegate shall designate the persons responsible for cybersecurity referred to in Article 15 of the Law on Cybersecurity and other persons responsible for the implementation of the requirements of the Regulation.

17. The head of the cybersecurity entity or his/her delegate shall ensure that the NCSC is informed of the designated cybersecurity officers through the CISA and is provided with the contact information specified in the CISA Regulations.

18. The staff of the cybersecurity entity shall be informed of the designated cybersecurity officers.

19. The Cybersecurity Manager and/or the Security Officer shall not perform functions related to the administration of the network or information system or other functions related to the maintenance and management of hardware or software.

20. The Cyber Security Manager and/or the Safety Officer shall have the following functions in coordinating and overseeing the implementation of the requirements set out in the cyber security policy documents:

20.1. organise the assessment of the compliance of the cybersecurity entity with the requirements of this Regulation in accordance with the procedure established by the methodology for conducting cybersecurity audits approved by the NCSC;

20.2. ensuring that the cybersecurity policy documents are prepared and periodically updated in accordance with the requirements of the Law on Cybersecurity and the implementing legislation;

20.3. coordinate investigations into cyber incidents involving the network and the information system and cooperate with the competent authorities investigating cyber incidents and unlawful acts related to cyber incidents;

20.4. to provide the network and information system administrator(s) and/or users with mandatory instructions and orders related to the implementation of the requirements set out in the cybersecurity policy documents;

20.5. organise and participate in the risk assessment process, prepare and submit risk assessment reports and risk management plans for approval by the head of the cybersecurity entity or his/her delegate;

20.6. organise training for staff on cyber security issues;

20.7. perform other functions defined in the cybersecurity policy documents and other legal acts regulating cybersecurity and assigned to it.

21. The head of the cybersecurity entity or his/her authorised person shall designate a responsible person (administratoriq) to supervise the networks and/or information systems and ensure their operation. The functions of this person shall include the management of access rights for users of the network and information system, the maintenance of the network and information system components (computer, operating system, database, applications, security wall, intrusion detection system), the set-up of the information system components, the identification of vulnerabilities in the information system, the identification and monitoring of compliance with security requirements and the monitoring and responding to cyber-incidents.

SECTION FOUR MANAGEMENT OF CYBER INCIDENTS

22. The head of the cybersecurity entity or his/her authorised person must approve a cyber incident management plan, which must comply with the provisions of the National Cyber Incident Management Plan approved by the Government of the Republic of Lithuania.

23. In cases where the cybersecurity entity is provided with network and information system services related to the management of cyber incidents by service providers, the cybersecurity entity's cyber incident management plan shall be coordinated with the service provider.

24. The cyber incident management plan shall specify:

24.1. cyber incident identification ffidai;

24.2. the assessment of the cyber incident;

24.3. the organisation of cyber incident management;

24.4. provisions for communicating cyber incidents with stakeholders;

24.5. the responsibilities of the staff responsible for managing cyber incidents;

24.6. provisions for the identification, collection, receipt, reporting and preservation of evidence of a cyber incident;

24.7. Assessment of lessons learned in cyber incident management;

24.8. Provisions for testing the effectiveness of the cyber incident management plan and for the preparation of a report on the outcome of the testing.

25. The cybersecurity entity shall establish r e q u i r e m e n t s for the administration and storage of logs, the detection and prevention of breaches, which shall include:

25.1. requirements for the storage, recording and periodic analysis of logs of the operating system, network and information system, technical equipment;

25.2. requirements for the periodicity of recording and analysis of traffic entering and leaving the network, antivirus s o f t w a r e, an intrusion detection and prevention system or the retention of secure human records;

25.3. requirements for the collection of access or modification actions for network and information system configuration and backup files.

26. The technical requirements applicable to cybersecurity entities are set out in Table 1.

1 Table 1

No.	**Technical requirements for cyber security entities**	**Essential**	**Essential**
1.	At least six logged events must be recorded (if the network or parts of the information system support such functionality):		
1.1.	the network and information system component (serveriq, virtualiq serveriq, (e.g., the server/server/service server, marirutizatoriq,	x	x

No.	Technical requirements for cyber-security entities	Essential	Essential
	switching and other entity identification of the criticalq components) switching, disconnecting or reconnecting;		
1.2.	user and administrator authentication events;	x	x
1.3.	creation of user and administrator accounts, access to changes to networks and information systems1¡;	x	x
1.4.	Actions to be carried out by the administrator;	x	x
1.5.	Scheduled task events created and executed on operating systems,	x	x
1.6.	Changes to group policies;	x	x
1.7.	amendments to the safety rules;	x	x
1.8.	Activation of the collection function of the jumbilical lists;	x	x
1.9.	Changes to the time and date of the operating system¡;		
1.10.	Connecting and disconnecting security systems (antivirus, intrusion detection);	x	x
1.11.	processes or service events in operating systems;	x	x
1.12.	network and information system equipment authentication failures;	x	x
1.13.	reviewing, deleting, modifying or changing the logbook.	x	x
2.	Networks and information systems shall have at least 2 time resources.	x	x
3.	At least the following data shall be recorded in log files (if the network and information system components support such functionality):		
3.1.	Date and exact time of the event;	x	x
3.2.	Event messages (information, error, safety message, system message, warning*);*	x	
3.3.	user/administrator/tínklq and identification data of the information system device associated with the trip;	x	x
3.4.	Description of the event.	x	x
4.	The pñemonies used in the interface between the internal network and the information system with the public electronic **communications** network shall be set up in such a way as to record in the log files all events related to incoming and outgoing data flows.	x	x
5.	The log files recorded by the network and the information system shall be stored in a specialised service suitable for hardware or software.	x	
6.	In the event of a {vairiiţ disturbance stopping the capture of data for auditing, the Cybersecurity Manager and/or the Safety Officer must be informed immediately (by automated *alert), but* within one working day at the latest.	x	

No.	Technical requirements for cybersecurity entities	Essential	Essential
7.	Human records must be kept for at least 90 calendar days.	x	x
8.	It is forbidden to delete or modify the journal entries before the expiry of the retention period of the journal entries.	x	x
9.	Copies of the logbooks shall be protected against damage, loss, unauthorised alteration or destruction.	x	x
10.	The use of the log files shall be controlled and recorded, and the log files shall be accessible only to persons authorised by the cybersecurity entity and the cybersecurity manager (with review rights).	x	x
11.	The data must be analysed by the authorised person at least once a month and the cybersecurity manager must be informed of the deviations in the analysed results a manager and/or safety jgaliot.	x	x
12.	Intrusion detection systems shall be in place and operational to monitor traffic in and out of the| network and information system.	x	x
13.	Unusual activity shall be recorded in the l o g s and, where possible, an automated message shall be generated by automated means and seen by the cybersecurity manager and/or the safety officer.	x	x
14.	The cybersecurity entity's internal network and information systems shall be separated from the public communications network using a firewall.	x	x
15.	The security rules of the firewall shall be kept under regular review and updated as necessary. A detailed analysis of the rules should be carried out at least once every 6 months.	x	x

SECTION FIVE
BUSINESS CONTINUITY

27. The head of the cybersecurity entity or his/her delegate must approve a business continuity management plan for the tínklq and the information system, which must include:

27.1. the conditions under which the business continuity plan for networks and information systems is triggered;

27.2. the performance criteria for determining whether the network and information system has been restored;

27.3. the persons responsible for the implementation of the network and information system business continuity plan, their duties and functions;

27.4. provisions which shall specify the requirements for the composition and functions of the network and information system business continuity management team, including the requirement that the business continuity management team shall include a cyber security manager and/or a security delegate;

27.5. provisions to specify the requirements for the composition and functions of the business resilience team for networks and information systems;

27.6. a detailed recovery plan for the network and information system;

27.7. the requirements for the development of an effective business continuity management plan for the network and information system;

27.8. requirements for the preparation of a report on the results of the performance testing of the business continuity management plan for the network and information system;

27.9. recovery parameters for the recovery of back-up data in accordance with the recovery *time objective* (RTO) for the network and information system, or part thereof, as defined by the cybersecurity entity, and the requirements for the testing of these parameters;

27.10. *the recovery point objective* (RPO) and its testing requirements for networks and information systems, or parts thereof.

28. The cybersecurity entity shall define the requirements for the backup, storage and recovery of data, and the extent and frequency of backup, taking into account the recovery point requirements (RTO, RPO) for networks and information systems set out in the business continuity management plan.

29. The cybersecurity entity shall submit the validation data of the report on the implementation of the business continuity management plan for the network and information system, indicating the date of the validation and the registration number, to the CISA at the latest within 5 working days after the validation of these documents.

30. The NCSC shall have the right to request the cyber security entity to provide a copy of the business continuity management plan validation report when carrying out an inspection of the cyber security entity. The cybersecurity entity shall submit these documents to the QIS within 5 working days of the receipt of the request by the NCSC.

31. The technical requirements for cybersecurity entities are set out in Table 2.

2 Table 2

No.	**Technical requirements for cyber security for cybersecurity entities**	**Essential**	**Essential**
16.	The availability of the network and information system assessed by the cybersecurity entity as critical t o business continuity must be ensured:		
16.1.	At least 96 % of the area;		x
16.2.	at least 99 % of the time.	x	
17.	Backup copies (hereinafter referred to as 'copies') of the data shall be made and retained in accordance with the procedures and at the intervals specified by the cybersecurity entity at a geographically remote location.	x	x
18.	The copies must be regularly tested by an authorised person or by the use of a specific software tool that automatically checks whether the data can be restored from a copy of the data that is fully functional.	x	x
19.	Provision shall be made for back-up premises to which network and information systems equipment can be temporarily relocated if it is not possible to continue operations in the main premises, and meet the r e q u i r e m e n t s of the main premises.	x	x
20.	The critical network and information system equipment, data network nodes and **communication** lines shall be duplicated and technically monitored at all times.	x	x

SECTION SIX SUPPLY CHAIN SECURITY

32. The head of the cybersecurity entity, or his/her delegate, shall establish supply chain security management procedures applicable to the procurement of services, works or equipment related to the design, development, installation, operation, maintenance, upgrading and/or cybersecurity of networks and information systems, in order to mitigate the risks that may be incurred by the network and the information systems.

33. The cybersecurity entity, in establishing its supply chain security management procedures, shall include criteria for the selection of network and information system suppliers, including:

33.1. the supplier's compliance with the cybersecurity requirements set out in the Description;

33.2. the qualitative requirements for network and information system products and services;

33.3. access management, including access time limitation.

34. The cybersecurity entity shall provide in its contracts with suppliers (including subcontractors), in relation to the services provided:

34.1. the supplier's compliance with the present Description;

34.2. the education and/or training and/or certification and/or qualifications required for the supplier's personnel;

34.3. the obligation of the supplier to notify the cybersecurity entity of any major and/or other incidents involving the cybersecurity entity's networks and information systems as soon as the supplier becomes aware of the incident, and to provide the cybersecurity entity with a report on the investigation of the cyber incident;

34.4. the right of the Cybersecurity Entity or its authorised service providers to audit the Supplier's compliance with the Description (including unscheduled audits) and the Supplier's obligation to facilitate such audits during the term of the Contract or in the event of a major incident,

34.5. the obligation to ensure the management of vulnerabilities posing a cyber security risk to the entity's networks and information systems;

34.6. confidentiality and non-disclosure obligations;

34.7. Security *Level Agreement* (*SLA*);

34.8. define the levels and conditions of access (login and physical) to the network and the information system;

34.9. provide for the requirements for the supplier's premises, equipment, network and information system access, and for the transmission of information over networks;

34.10. provide for the rights and obligations of the supplier and the cybersecurity entity.

35. The cybersecurity entity shall, when adopting the supply chain security management procedure, include requirements for risk assessment of network and information system providers.

36. The cybersecurity critical entity shall have a contract(s) with the provider of the Internet service, if the data transmission service is essential for the provision of the service, which shall provide for the following:

36.1. response to cyber incidents during normal working hours;

36.2. after-hours response to cyber incidents;

36.3. uninterrupted provision of Internet service: 24 hours a day, 7 days a week;

36.4. service disruption logging: 24 hours a day, 7 days a week;

36.5. *Denial of service (*DoS) protection.

37. The relevant cybersecurity entity must have entered into an agreement(s) with the provider of the Internet service, if the data transmission service is essential for the provision of the service, which must provide for:

37.1. response to cyber incidents during normal working hours;

37.2. uninterrupted provision of the service during normal working hours;

37.3. logging of service disruptions during normal working hours;

37.4. application of network and information system disruption (DoS) protection.

38. The cybersecurity entity shall monitor the implementation of the cybersecurity requirements specified in the contract with the supplier.

39. The cybersecurity entity shall maintain a list of suppliers and review and update it as contracts change, at the scheduled intervals and when necessary changes or incidents involving the suppliers occur.

SECTION SEVEN
SECURITY IN THE ACQUISITION, DEVELOPMENT AND MAINTENANCE OF NETWORKS AND INFORMATION SYSTEMS, INCLUDING VULNERABILITY MANAGEMENT AND DISCLOSURE

40. The head of the cybersecurity entity, or his/her delegate, shall establish procedures to ensure the security of the acquisition, development and maintenance of networks and information systems, which shall include:

40.1. the requirements for the acquisition and installation of the network and information system;

40.2. the provisions for the use of the security system to protect networks and information systems against malicious software (virus, inipinêjjem software, spam, etc.) and the requirements for updating it;

40.3. the basic use of computer network filtering equipment (security, content control, proxy, etc.);

40.4. security measures to secure the data transmission network;

40.5. secure use of e-mail;

40.6. provisions on the approval of the list of permitted software, the regularity of its review at least once a meme and its updating;

40.7. other measures used to ensure cybersecurity.

41. Software shall be installed only by persons authorised by the cybersecurity entity. Users of the system shall not be authorised to install the software on their own.

42. The cybersecurity entity shall establish procedures for managing changes to the network and information system (hereinafter referred to as 'changes'), including planning, identifying the change, categorising the change according to the type of change, assessing the impact and prioritising the change.

43. Any changes that could disrupt or stop the operation of the cybersecurity entity must be agreed with the head of the cybersecurity entity or his/her delegate and must be tested in a test environment.

44. The cybersecurity entity shall establish patch management procedures. Security patches shall be tested prior to deployment in a production environment. Official manufacturer security patches shall be deployed and integrity testing shall be performed prior to deployment. Security fixes shall not be implemented if they contain vulnerabilities that may cause more harm than the benefits of implementation.

45. The head of the cybersecurity entity, or his/her delegate, shall adopt a vulnerability management and disclosure policy that shall specify:

45.1. Identification and assessment of vulnerabilities that may have an impact on cybersecurity;

45.2. the rights and obligations of those responsible for identifying the vulnerability;

45.3. the development of a plan to identify the vulnerability;

45.4. Use of vulnerability detection software;

45.5. classification of the results of the vulnerability detection;

45.6. Preparation of the report on the identification of gaps and the identification of trükumq;

45.7. the requirement to immediately close a vulnerability assessed as critical to the operation of the network and information system;

45.8. the requirement for regular vulnerability assessments and a full vulnerability scan of the networkq information system at least every 6 months;

45.9. investigation and reporting of vulnerabilities reported under Article 25 of the Law on Cyber Security.

46. The handling of gaps shall be in accordance with the provisions on change and incident management of the cybersecurity entity.

47. The technical requirements for cybersecurity entities are set out in Table 3.

3 Table 3

No.	**Technical requirements for cybersecurity entities**	**Essential**	**Essential**
21.	The cybersecurity entity must have an up-to-date networking and infonnaciniq system the logical diagram of the infrastructure and the diagrams of the entire network and information system (to be updated as they change).	x	x
22.	|The *attack* signature shall be updated using trusted sources of current information. The latest hacking attack signatures shall be installed no later than 24 hours from the date of the manufacturer's announcement of the latest hacking attack signatures, or no later than 72 hours from the date of the manufacturer's announcement of the latest hacking attack signatures, if the cybersecurity entity decides to carry out an assessment (testing) of the implementation of the hacking attack trace and its possible impact on the cybersecurity entity's operations.	x	
23.	Servers (including virtual machines) and workstations shall be equipped and configured with a security system that controls all jcinanti and iàcinanti traffic.	x	x
24.	Emails received from outside must be filtered to detect and block malicious content.	x	x
25.	Configuration rules for technical and software equipment for the detection of cyber incidents shall be stored in electronic form separately from the technical equipment for the network and the infonnacînip system (with the relevant dates (implementation, update), responsible persons, application periods).	x	x
26.	When connecting to a wireless network (if connecting to the internal n e t w o r k of the network and the information system), the *Extensible Authentication Protocol* (EAP) and the *Transport Layer Security* (TLS) protocol, or a newer protocol generally recognised as secure, shall be applied to authenticate the user of the network and information system.	x	x
27.	The network shall be managed using secure network protocols.	x	x
28.	All unlisted protocols and open ports shall be disabled / disabled.	x	x
29.	*Peer to peer* shall be enabled on computers, mobile devices functionality where it is no longer necessary for the performance of job functions.	x	
30.	Updates recommended by the manufacturer of the software used and the operating system shall be installed.	x	x
31.	Network and information systems using unsupported versions of the operating system and other software for objective reasons shall operate on a separate network segment from the core business function of the cybersecurity entity.	x	x
32.	The internal computer network of the cybersecurity entity must be segmented to include at least:		
32.1.	The network and information system management and administration subnetwork;	x	x

No.	Technical requirements for cybersecurity entities	Essential	Essential
32.2.	a separate subnetwork for each third party, or otherwise ensuring that the third party has access only to the resources required by that party, where possible by means of multi-factor login authentication. The connection shall be made using a secure virtual private *network* (VPN). The connection shall be logged in the logging logs;	x	x
32.3.	the networked multifunctional device and the printer and scanner subnetwork;	x	x
32.4.	IP telephony potinklț;	x	x
32.5.	Workplace potinklq;	x	x
32.6.	testing potinkl).	x	x
33.	Mobile devices and computer workstations shall have *executable* code controls to restrict the use of unauthorised executable code or to notify the administrator of the use of unauthorised executable code.	x	x
34.	Operating system images and/or other tools with built-in security provisions shall be developed and deployed for computer workstations (including non-removable devices). The image shall contain only the components of the operating system that are necessary for the operation (administrative accounts, services, applications, network ports, updates, system tools). The images must be regularly reviewed and updated, and immediately updated when a new vulnerability or attack is detected. The images shall be used to install an operating system with security provisions on ¡ computer workstations (including non-removable devices).	x	x
35.	It is forbidden to store session data (identifiers) on the website servers for the purpose of logging in after the end of the merging session.	x	x
36.	A *Web Application Firewall* (WAF) must be used for Internet-accessible websites, networks and information systems.	x	x
37.	Internet-accessible websites, networks and information systems shall be protected against basic network-based attacks based on the *Open Web Application Security Project (*OWASP) Top 10 Best Practices (www.owasp.org) .	x	x
38.	Web forms shall use input validation.	x	x
39.	Web-accessible networking and information systems must not display error messages to the user about the networking and information system and software code or server	x	x
40.	Network and information system security measures available over the Internet using *HyperText Transfer Protocol Secure (*HTTPS) must allow only the functionality of jq the protocol methods required to ensure the availability of the jq service.	x	x
41.	The cybersecurity entity's servers and workstations shall employ (centrally managed and updated, if possible) real-time malware detection, monitoring and monitoring tools.	x	x
42.	Only legal and permissible (according to a list approved by the cybersecurity entity) software shall be used.	x	x
43.	The amount of available memory or disk space on the network and information system equipment shall be monitored on a continuous basis, as well as load and resource usage. When the limits are reached, the responsible persons shall be informed.	x	x

SECTION 8
ASSESSING THE EFFECTIVENESS OF CYBERSECURITY REQUIREMENTS

48. The head of the cybersecurity entity or his/her delegate shall establish a procedure for assessing the effectiveness of the cybersecurity requirements, including:

48.1. a requirement to regularly, at least annually, assess the compliance of the cybersecurity entity with the Cybersecurity Law, the requirements set out in the Cybersecurity Law, the Cybersecurity Description and the cybersecurity policy documents adopted by the cybersecurity entity (hereinafter referred to as "Compliance Assessment").

48.2. Following the completion of the Compliance Assessment by the Cybersecurity Entity, the Compliance Assessment shall be prepared and reviewed by the Head of the Cybersecurity Entity or his/her delegate:

48.2.1. Compliance Assessment Report;

48.2.2. a plan for the resolution of the identified non-conformities (if any), which shall identify the responsible actors, the resources required and the timeframe for implementation.

48.3. the requirement to carry out a cyber-security audit on a regular basis, at least once every 3 years, in accordance with the provisions of Article 14(8) of the Law on Cybersecurity;

49. The cybersecurity entity shall, taking into account the results of the risk assessment, the occurrence of cybersecurity incidents and the results of the management of the jq, establish the requirements for the assessment of the effectiveness of the cybersecurity measures:

49.1. which cybersecurity requirements management measures need to be monitored and evaluated;

49.2. which monitoring, measurement, analysis and evaluation methods the cybersecurity entity shall apply;

49.3. the frequency with which the monitoring and measurement of the identified methods should be carried out;

49.4. those responsible for monitoring and measuring the effectiveness assessment;

49.5. the periodicity of the analysis of the results of the performance evaluation;

49.6. the improvements to be made to cybersecurity measures in the light of the results of the evaluation.

50. The NCSC, when conducting an inspection of a cybersecurity entity, shall have the right to require the cybersecurity entity to submit copies of the cybersecurity audit, the compliance assessment report, the plan for addressing non-compliance identified during the compliance assessment, the risk assessment report and the risk management plan. The cybersecurity entity must submit these documents to the CISA no later than 5 working days from the date of receipt of the NCSC's request.

51. The cybersecurity critical entity shall provide a cybersecurity compliance assessment at least once a year by completing the NCSC questionnaire in the CISA.

SECTION NINE
CYBER HYGIENE PRACTICES AND CYBERSECURITY TRAINING

52. The head of the cybersecurity entity or his/her delegate shall establish procedures for the organisation and conduct of cyber hygiene practices and cybersecurity training. The head of the cybersecurity entity must ensure that all employees of the cybersecurity entity receive cyber hygiene training at least once a year.

53. The cybersecurity entity shall ensure that employees are informed about cybersecurity issues (training and information methods shall be chosen according to the specific nature of the network and information system).

54. Within three months after the cyber security training, a training report must be prepared, including the subject of the training and the number of participants. The cybersecurity entity shall have the right to procure training on the specified topics from third parties or to organise it itself. The cybersecurity entity must keep the report on the training for at least three years from the date of approval of the report.

SECTION TEN
POLICIES AND PROCEDURES FOR THE USE OF CRYPTOGRAPHY AND ENCRYPTION

55. The head of the cybersecurity entity, or his/her delegate, shall establish procedures for the use of cryptography and encryption, including:

55.1. the cybersecurity entity's provisions for the use of cryptography and encryption tools, taking into account the| cybersecurity entity's requirements for the classification and handling of information;

55.2. key management (generation, destruction, archiving, etc.).

56. In the event of loss of a cryptographic key, the responsible person shall be informed.

57. The technical requirements for cybersecurity entities are listed in Table 4.

4 Table 4

No.	Technical requirements for cybersecurity entities	Essential	Essential
44.	The confidentiality of sensitive information transmitted to a cybersecurity entity over public electronic communications networks shall be ensured by the use of encryption or a virtual *private network* (VPN).	x	x
45.	Wireless communications shall be encrypted with an encryption key length recommended by good security practice. Use keys and protocol versions recognised as generally secure. Standard manufacturer's keys shall be replaced at the wireless access station.	x	x
46.	the moments transmitted between the mobile device and the network and the information system must be encrypted using Virtual Private Network (VPN) technology with TLS/SSL certificate or using *Access Point Name (*APN) technology through the mobile operator, with in-stream data encryption with a TLS/SSL certificate when the VPN technology is not supported on the mobile device.	x	x
47.	Network and information system data stored on mobile devices and on computer storage media shall be encrypted.	x	x
48.	Website cryptography requirements shall be implemented:		
48.1.	Officially recognised secure key lengths must be used;	x	x
48.2.	Communications shall be encrypted for site administration;	x	x
48.3.	The digital certificates used for encryption must be issued by a trusted certificate authority;	x	x
48.4.	The TLS standard (version 1.3 or higher) must be used;	x	
48.5.	the cryptographic functions of the website must be implemented in the server on which the website is hosted or in a cryptographic security module (*Hardware security module)*;	x	x
48.6.	All cryptographic modules shall be able to *fail securely.*	x	
49.	The data in the backup copies must be encrypted (the encryption keys must be kept separate from the copies) or other measures must be taken to prevent the copies from being used for unauthorised reproduction of information.	x	x
50.	Audit trails relating to cryptographic key management activities (generation, destruction, archiving, user actions) shall be maintained and monitored.	x	x

SECTION ELEVEN

HUMAN RESOURCES, PROTECTED RESOURCES, PHYSICAL ACCESS POLICY AND ASSET MANAGEMENT

58. The head of the cybersecurity entity, or his/her delegate, shall establish human resources security requirements, which shall include:

58.1. a requirement that access to the cybersecurity entity's network and information system shall only be granted to the cybersecurity entity's employees and/or service providers after they have read and agreed to abide by the cybersecurity policy documents;

58.2. confidentiality or non-disclosure requirements for employees and/or service providers of the cybersecurity entity.

59. The head of the cybersecurity entity or his/her delegate shall approve the physical access requirements for networks and information systems, including:

59.1. a list of the premises to be protected (premises housing the cybersecurity entity's network and information systems equipment, servers, user and administrator workstations);

59.2. the physical environmental protection and access control measures to be applied to the protected premises;

59.3. the requirement that only authorised persons may enter the premises protected by the cybersecurity entity;

59.4. the designation of a person responsible for the implementation of the physical protection measures.

60. The technical requirements applicable to cybersecurity entities are set out in Table 5.

5 Table 5

No.	Technical requirements applicable to cybersecurity entities
51.	The network and information system premises and the premises where backup data are stored shall be protected against unauthorised access by physical or electronic security measures.
52.	Access to the network and information system server rooms and premises where backups are stored shall be controlled in accordance with procedures established by the cybersecurity entity.

61. The head of the cybersecurity entity or his/her delegate shall establish procedures for the management of the assets of the cybersecurity entity, including:

61.1. the requirement to establish and keep up-to-date a list of network and information system assets (hardware, software, data) under the control of the cybersecurity entity that support the cybersecurity entity's operational functions (hereinafter referred to as the 'asset list');

61.2. the requirements for classifying assets in terms of jq relevance, confidentiality, integrity and availability;

61.3. requirements for the transfer of assets outside the boundaries of the cybersecurity entity; ó1.4. requirements for the use of non-salvageable, replaceable data storage media;

61.5. the requirements for the secure use and control of mobile devices that can operate independently and communicate with the network or the Internet as their location changes (e.g. laptop, handheld, mobile phone) and are used to connect to the cybersecurity entityq network and information system.

62. The maintenance and troubleshooting of the network and information system equipment shall be carried out by qualified professionals.

63. Network and information system hardware failures shall be logged.

64. The technical requirements for cybersecurity entities are set out in Table 6.

6 Table 6

Nr.	Technical requirements applicable to cyber security for entities *1	Essential	Essential
53.	Technical measures shall be in place to restrict the connection of unauthorised (non-listed) equipment to the cybersecurity entity's network and information system, to restrict the use of unauthorised equipment and to inform the cybersecurity entity's authorised person).	x	x
54.	The cybersecurity entity shall centrally manage mobile devices that have access to the network and information system and the software installed on them.	x	x
55.	Mobile devices used to browse the Internet must be protected against threats posed by mobile *code*.	x	
56.	Mobile devices must be equipped with means to allow remote, irretrievable erasure of data on mobile devices.	x	
57.	Requirements for hardware, software and facilities for the network and the infotainment system:		
57.1.	network and information system, computer equipment that has been assessed as critical by the cybersecurity entity shall be equipped with a voltage filter and an uninterruptible power supply to ensure the operation of the hardware;	x	x
57.2.	if the network and the information system are hosted indoors the combined capacity of the equipment in the information and data centre room is more than 10 kilowatts, an air-conditioning equipment shall be provided;	x	x

57.3.	air-conditioning and drêgmés control equipment shall be installed in the server room;	x	
57.4.	the hardware and software for the network and information system 4.4.4. the information and communication system equipment must be maintained in accordance with the manufacturer's recommendations;	x	x
57.5.	Fire and smoke detectors shall be p r o v i d e d in the network and information system server rooms and shall be connected to the building's alarm/security service monitoring panel;	x	x
57.6.	all premises where the cybersecurity entity's hardware is located shall be equipped with fire detectors a n d / o r other physical protection measures;	x	
57.7	Critical elements (air-conditioning, ventilation and drégmés control, power supply) shall be duplicated in order to ensure a high level of availability of the premises reliability of the equipment.	x	

SECTION TWELVE

CONTROL OF APPLIANCES AND MEASURES FOR DETERMINATING THE PATHWAY,J PERFORMANCE

65. The head of the cybersecurity entity, or his/her delegate, shall establish access management procedures that include:

65.1. the establishment of the cybersecurity entity's user, administrator and service provider groups, the granting and management of rights and access to the cybersecurity entity's networks and information systems;

65.2. the levels of access to the network and information system by the administrator(s) and the cybersecurity requirements applicable to them (reading, creating, updating, destroying, editing of information used by the network and information system, access rights, etc.);

65.3. the requirements for registration and deregistration of the user of networks and information systems and the person responsible for carrying out this action

65.4. the means to identify the user of the network and information systems;

65.5. the requirements for the creation, validity and change of passwords for the user and administrator of the network and information system:

65.5.1. the requirement that personal information (for example, date of birth, names of family members, etc.) must not be used to create passwords;

65.5.2. the requirement that the password must not be composed of a repeating or sequential character (e.g. "aaaaaaaaaaa" or "0123456789") or a common keyboard sequence (e.g. "Qwerty");

65.5.3. a prohibition on the use of manufacturer-specified passwords in hardware and software, which must be changed in accordance with the requirements set out in this section;

65.6. the prohibition to disclose passwords to other persons;

65.7. the conditions and cases under which the right of a user and administrator of a network and information system to work with specific information is revoked;

65.8. the permissible conditions for remote access to the network and information system by the user and the administrator;

65.9. the conditions for the use of the various authentication tools.

66. The cybersecurity entity shall approve a list of persons granted administrator rights to access the network and information system, which shall be reviewed periodically by the person responsible for cybersecurity. The list shall be revised when the administrator is removed or his/her employment/service relationship ends.

67. Passwords shall not be stored or transmitted in clear text. Only a password in clear text may be transmitted in clear text, but separately from the login name, if the users do not have the possibility to decrypt the encrypted password received or if there is no technical possibility to transmit the password to the user via an encrypted channel or a secure electronic communication network.

68. The head of the cybersecurity entity or his/her delegate shall approve the use of a multi-actor authentication or persistent authentication solution, secure voice, video and text communications, and a secure emergency communications system within the entity.

69. The technical requirements for cybersecurity entities are set out in Table 7.

7 Table 7

№	Technical requirements applicable to cybersecurity entities	Essential	Essential
58.	Administrator functions shall be performed using a separate dedicated account for the service, which shall not be used for day-to-day user functions.	x	x
59.	Users shall not be granted administrator privileges.	x	x
60.	Each user shall be uniquely identifiable.	x	x
61.	The user and the administrator shall authenticate themselves with a password and an additional authentication means (multiple authentication means).	x	x
62.	A user's right to work with a particular network and information system shall be suspended when the user has not used the network and information system for more than 3 months.	x	x
63.	The administrator's right to work with a network and information system shall be suspended when the administrator does not use the network and information system for more than 2 months.	x	x
64.	When a user or administrator is removed from his/her employment (position), does not meet the requirements for the qualification of a user or administrator as set out in other legal acts, or when his/her employment (service) relationship is terminated, or when he/she loses his/her security clearance, his/her right to use the network and the information system shall be revoked immediately, but at the latest within the time limit set by the cybersecurity entity.	x	x
65.	Unnecessary or unused network and information system accounts shall be blocked immediately, but no later than within a timeframe determined by the cybersecurity entity, and deleted after the expiration of the retention period retention periods (at least 90 calendar days).	x	x
66.	Upon completion of work or when leaving the workplace, the network and information system shall be disconnected and the screen saver with the passcode shall be activated.	x	x
67.	The workstation shall lock (after no more than 15 minutes) when no action is being taken on the networks and information systems, so that further use of the network and information system is only possible after reauthentication.	x	x
68.	The parts of the network and information system, including the websites and browsers that authenticate the user, shall prohibit the storage of passwords by specialised password management software.	x	x
69.	The password shall be composed of upper and lower case letters, numbers and special characters.	x	x
70.	The maximum number of times that the user may log on to the tínk1q and information systems shall be set at a maximum of 5 times per line. After the default	x	x

No.	Technical requirements for cybersecurity entities	Essential	Essential
	The number of attempts to connect to the network and the information system account shall be blocked. Only the following may unblock authorised persons.		
71.	Additional user password requirements:		
71.1.	The password must be changed at least every 6 months;	x	x
71.2.	The password must be at least 10 characters long;	x	x
71.3.	the password to be changed shall not be allowed to consist of the previous 6 most recent passwords;	x	x
71.4.	the user shall be required to change his/her password on first connection to the network and information system;	x	x
71.5.	the user shall be able to change his password at any time.	x	x
72.	Additional administrator password requirements:		
72.1.	The password shall be changed at least every 6 mėnesius;	x	x
72.2.	The password shall be at least 15 characters;	x	x
72.3.	When changing the password, the password from the previous 8 last passwords shall not be allowed.	x	x
73.	The administrator account shall be monitored:		
73.1.	Regularly, at least once a year, check that administrator accounts comply with the requirements set out in this section and report to the Authorised Person in Charge administrator accounts that do not comply with the requirements set out in this section;		x
73.2.	the use of administrator account controls that periodically check administrator accounts. Administrator accounts that do not comply with the requirements set out in this Section shall be notified to the authorised person.	x	
74.	Control of user accounts shall be carried out:		
74.1.	User accounts shall be regularly checked for compliance with the requirements set out in this Section. User accounts that do not comply with the requirements set out in this section shall be reported to the authorised person;		x
74.2.	means shall be in place to control user accounts, which shall periodically check user accounts. User accounts that do not comply with the requirements set out in this Section shall be reported to the authorised person person.	x	
75.	Local user and administrator passwords shall comply with the requirements set out in this section.	x	x
76.	Additional requirements for authentication, authorisation and access control (for cybersecurity entity websites accessible from a public electronic connection)		

No.	Technical requirements for cybersecurity for cybersecurity entities	E..i.i.s	Important
	tinklų):		
76.1.	The program code shall not contain data (name, passwords, application programming interfaces (APIs*), keys (*tokens*)*, etc.) that, if disclosed, could be used to gain access to devices, resources, accounts or a device, application or account.	x	x

CHAPTER III FINAL PROVISIONS

70. The implementation of the requirements of the Regulation shall not relieve the cybersecurity entity{ from the obligation to implement the requirements laid down in other legal acts aimed at ensuring the security of networks and information systems, except in the cases provided for in Section 1(3) of the Law on Cybersecurity.

71. Cybersecurity entities must implement the cybersecurity requirements within 12 months of their registration in the Cybersecurity Information System, except as provided for in point 72 of the Regulation.

72. Cybersecurity entities must implement the technical cybersecurity requirements set out in points 26, 31, 47, 57, 60, 64, 69 of the Annex no later than 24 months from the date of registration in the Cybersecurity Information System.

APPROVED BY
by the Government of the Republic of Lithuania
by Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018
(Government of the Republic of Lithuania wording of Decree No 945 of 6 November 2024)

DESCRIPTION OF THE PROCEDURE FOR THE APPLICATION OF THE USE OF CIVERBER SECURITY SUBJECTS

CHAPTER I
GENERAL PROVISIONS

1. The Rules of Procedure on the Application of Enforcement Measures to Cybersecurity Entities (hereinafter referred to as "the Rules") shall govern the selection of enforcement measures, the application of enforcement measures in the event of multiple breaches and the imposition of penalties on cybersecurity entities.

2. The terms used in the Regulation shall be understood as defined in the Law on Cyber Security of the Republic of Lithuania.

CHAPTER II
SELECTION OF ENFORCEMENT MEASURES

3. The selection of enforcement measures shall consist of ii:

3.1. An assessment of the circumstances referred to in Article 28(3) to (5) of the Law on Cybersecurity. The assessment of the circumstances referred to in Article 28(3)(2) to (9) of the Cybersecurity Act shall take into account the positive and negative aspects of the circumstances, in accordance with the procedure set out in point 4 of the Regulation;

3.2. Choice of enforcement measure(s), taking into account the appropriateness of the enforcement measure(s).

4. The assessment of the circumstances referred to in Article 28(3)(2) to (9) of the Law on Cybersecurity shall be carried out by identifying the positive and negative aspects of such circumstances:

4.1. Assessment of the circumstances referred to in Article 28(3)(2) of the Cybersecurity Law:

4.1.1. A positive assessment shall be made if the duration of the breach has been reduced due to the optimal and risk-free actions of the cybersecurity entity.

4.1.2. A negative assessment shall be made for breaches whose duration increases the risk of damage and adverse effects, makes it more difficult to reverse the damage or adverse effects, or impedes the ability of the National Cyber Security Centre to respond appropriately to the breach.

4.2. Assessment of the circumstances referred to in Article 28(3)(3) of the Cybersecurity Law:

4.2.1. A positive assessment shall be made if there has been no breach in the last two years.

4.2.2. A negative assessment shall be made for breaches committed by the cybersecurity entity in the last two years. The longer the time period between the previous breach and the breach currently under investigation, the less important this circumstance is for the imposition of an enforcement measure.

4.3. Assessment of the circumstance referred to in Article 28(3)(4) of the Cybersecurity Law:

4.3.1. A positive assessment is made where the damages have been repaired or the negative impact caused has been reversed at the initiative of the cybersecurity entity.

4.3.2. Failure to compensate for the loss or to eliminate the negative impact caused is assessed negatively.

4.4. Assessment of the circumstance referred to in Article 28(3)(5) of the Cybersecurity Law:

4.4.1. The existence of cybersecurity measures in place at the start of the inspection and notified to the cybersecurity entity at the start of the inspection by the National Cybersecurity Centre, the existence of cybersecurity measures that have been successful in preventing or minimising material or non-material damage, as well as the timely application of these measures, shall be assessed positively.

4.4.2. Failure by a cybersecurity actor to take measures to prevent or mitigate material or non-material damage shall be assessed negatively.

4.5. Assessment of the circumstance referred to in Article 28(3)(6) of the Cybersecurity Law:

4.5.1. A positive assessment shall be made if the cybersecurity entity has notified the breach in a timely and appropriate manner to the entities that should have received such information in accordance with the established codes of conduct or approved certification mechanisms.

4.5.2. A negative assessment shall be given where the cybersecurity entity has not complied with the codes of conduct or approved certification mechanisms and this is directly related to the breach.

4.6. Assessment of the circumstance referred to in Article 28(3)(7) of the Cybersecurity Law:

4.6.1. A positive assessment shall be made where the cybersecurity entity has responded to the requirements of the National Cyber Security Centre during the course of the inspection and the inspection has therefore been carried out more quickly and efficiently, and a positive assessment shall be made where the cybersecurity entity has acknowledged the breach by self-reporting the breach prior to the National Cyber Security Centre becoming aware of it.

4.6.2. It is negative when the cybersecurity actor's systematic9 and repetitive behaviour has delayed the verification or other surveillance activities.

4.7. Assessment of the circumstance referred to in Article 28(3)(8) of the Law on Cybersecurity:

4.7.1. A positive assessment shall be made when the scale of the breach referred to has been reduced due to optimal and risk-free actions by the cybersecurity entity.

4.7.2. A negative assessment shall be made where the breach has the potential to affect the operation of a vital service, and where the breach relates to essential network information systems owned and operated by the cybersecurity entity.

4.8. Assessment of the circumstances referred to in Article 28(3)(9) of the Cybersecurity Law:

4.8.1. The neutral factor is considered to be when the breach is due to negligence.

4.8.2. Deliberate infringements are frowned upon.

5. The enforcement measure(s) shall be chosen taking into account the appropriateness of the enforcement measure(s) after having assessed the circumstances referred to in Article 28(3) to (5) of the Law on Cybersecurity:

5.1. If the assessment of the breach of the Law on Cyber Security (hereinafter referred to as 'the breach') and its circumstances determines that it is not appropriate to impose an enforcement measure specifying specific measures to be applied or restricting the activities of the cyber security entity, one or more of the enforcement measures referred to in points (1)(1) and/or (3) of Article 28(1)(i)(ii) of the Law on Cyber Security shall be applied to enforce the requirements of the Law on Cyber Security.

5.2. If the assessment of the breach and its circumstances determines that it is appropriate to impose an enforcement measure to comply with the requirements of the Law on Cybersecurity to address the breach and/or the factors and causes of the breach, one or more of the enforcement measures referred to in Article 28(1)(2), (4), (6) and/or (7) of the Law on Cybersecurity shall be imposed.

5.3. If the assessment of the breach and its circumstances determines that it is appropriate to inform the public or certain groups of the public about the breach, one or more of the enforcement measures referred to in Article 28(1)(5) and/or (8) of the Law on Cyber Security shall be applied.

5.4. If the assessment of the breach and its circumstances determines that the enforcement measure referred to in Article 28(1)(1)-(8) and/or (10), (11) of the Law on Cybersecurity will not have a dissuasive effect on the offending cybersecurity entity, or that the dissuasive effect will be insufficient, the enforcement measure(s) referred to in Article 28(1)(1) to (8) and/or (10), (11) of the Law on Cybersecurity shall be applied together with the enforcement measure provided for in Article 28(1)(9) of the Law on Cybersecurity. The assessment of the deterrent effect shall assess whether the benefit to the cybersecurity entity from the continuation of the breach outweighs the impact of the enforcement measure and whether the application of the enforcement measure against the cybersecurity entity for previous breaches has achieved positive objectives.

CHAPTER III
APPLICATION OF ENFORCEMENT MEASURES IN THE EVENT OF SEVERAL BREACHES

6. If an inspection reveals a number of infringements, enforcement measures are applied immediately:

6.1. Where there are several infringements arising from separate acts or omissions, enforcement measures shall be applied separately for each infringement.

6.2. Where there are several infringements arising from a single act or omission, the enforcement measures shall be applied individually, provided that the application of a legal provision to a single infringement does not preclude or exclude the applicability of another legal provision.

6.3. Where there are several infringements arising from a single act or omission, the enforcement measure shall be applied for the more serious infringement, as defined in Article 29 of the Law on Cybersecurity, if the application of the legal provision to a single infringement precludes the applicability of, or is covered by, the other l e g a l provision.

CHAPTER IV
IMPOSING FINES ON CYBERSECURITY ACTORS

7. If a fine is chosen as one of the enforcement measures, the question of imposing a fine shall be considered and a decision on imposing a fine shall be taken in accordance with the procedure laid down in Article 31 of the Law on Cybersecurity.

AFFIRMED
The Government of the Republic of Lithuania
by Resolution No. 818 of the Government of the
Republic of Lithuania of 13 August 2018
(Government of the Republic of Lithuania
Resolution No. 945 of the Republic of Lithuania of
6 November 2024)

LIST OF USERS OF THE SECURE STATE DATA TRANSFER NETWORK

Efl. No.	**Name of the legal** entity
	Area of management of the Minister for the Environment of the Republic of Lithuania
1.	Ministry of the Environment of the Republic of Lithuania
2.	Environmental Protection Agency
3.	Lithuanian Geological Survey under the Ministry of Environment
4.	Lithuanian Hydrometeorological Agency under the Ministry of Environment
5.	State Territorial Planning and Construction Inspectorate under the Ministry of Environment
6.	Department of Environmental Protection under the Ministry of the Environment
7.	State Forestry Service
8.	National Land Management under the Ministry of Environment
9.	Environmental Project Management Agency of the Ministry of the Environment
i0.	Public body Construction Sector Development Agency
	Area of management of the Minister of Energy of the Republic of Lithuania
1i.	Ministry of Energy of the Republic of Lithuania
12.	State Enterprise Ignalina Nuclear Power Plant
13.	Public body Lietuvos energetikos agentüra
14.	State Energy Regulatory Council
	Area of management of the Minister of Finance of the Republic of Lithuania
15.	Ministry of Finance of the Republic of Lithuania
16.	State Enterprise Turto bankas
17.	Audit, Accounting, Asset Valuation and Insolvency Management Agency under the Ministry of Finance
18.	State Data Agency
19.	Lośimq Supervisory Authority under the Ministry of Finance
20.	Customs Department under the Ministry of Finance
21.	Kaunas territorial customs office
22.	Claípêda Territorial Customs Office
23.	Customs Information Systems Centre
24.	Customs Criminal Investigation Service
25.	Customs Laboratory
26.	Customs Training Centre
27.	Vilnius Territorial Customs Office
28.	National Centre for Bendnjjq Functions
29.	State Security Agency for Technological Protection of Documents under the Ministry of Finance
30.	State Tax Inspectorate under the Ministry of Finance
31.	Kaunas County State Tax Inspectorate
32.	Klaipėda County State Tax Inspectorate
33.	State Tax Inspectorate of Panevezys County

Eü. No.	Name of the legal entity
34.	Éiauliq County State Tax Inspectorate
35.	Vilnius County State Tax Inspectorate
	Area of management of the Minister for National Defence of the Republic of Lithuania
36.	Ministry of National Defence of the Republic of Lithuania
37.	Second Operative Department under the Ministry of National Defence
38.	Centralised Financial and Asset Assets Assignment under the Ministry of National Defence
39.	General Jonas Zemaiüis Lithuanian Military Academy
40.	Defence Resources Agency under the Ministry of National Defence
41.	Infrastructure Management Agency
42.	Bendnjq Reíkalq Department of the Ministry of National Defence
43.	Lithuanian Armed Forces
44.	Department of Mobilisation and Civil Resistance under the Ministry of National Defence
45.	National Cyber Security Centre under the Ministry of National Defence
46.	Vytautas Magnus War Museum
	Sphere of responsibility of the Minister for Culture of the Republic of Lithuania
47.	Ministry of Culture of the Republic of Lithuania
48.	Department of Cultural Heritage under the Ministry of Culture
49.	Lithuanian National Art Museum
50.	Lithuanian National Martynas Maivydas Library
51.	Lithuanian National Radio and Television
	Area of responsibility of the Minister for Social Security and Labour of the Republic of Lithuania
52.	Ministry of Social Security and Labour of the Republic of Lithuania
53.	Agency for Youth Affairs
54.	Centre for the Promotion of Youth
55.	Employment Agency under the Ministry of Social Security and Labour
56.	State Labour Inspectorate of the Republic of Lithuania under the Ministry of Social Security and Labour
57.	Agency for the Protection of Persons with Disabilities under the Ministry of Social Security and Labour
58.	Department of Social Services at the Ministry of Social Security and Labour
59.	State Committee for the Protection of the Rights of the Child and Child Protection under the Ministry of Social Security and Labour
60.	State Social Insurance Fund Board under the Ministry of Social Security and Labour
61.	Kaunas Division of the State Social Insurance Fund Board
62.	Klaipėda Division of the State Social Insurance Fund Board
63.	Panevê2io Division of the State Social Insurance Fund Board
64.	Vilnius Division of the State Social Insurance Fund Board
65.	Technical Assistance Centre
66.	Adakavo Social Services Home
67.	Aknysta social care home
68.	Düseikiq social care home
69.	Ilguva social care home
70.	Jurdaicip social care home
71.	Jotaíniq socialinés care home
72.	Jasiuliskip socialinés care home
73.	Kêdainiq socialinés orphanage
74.	Kupiskio socialinés foster home
75.	Lavênq socialinês care home
76.	Linkuva social care home
77.	Macikt¡ social care home
78.	Marijampolês Special Social Care Home
79.	Prüdiikiit socialinés care home
80.	Nijolês Genytês social care home
8 i.	Padvariq socialinés care home
82.	Suvalkija social care home
83.	Strêvininkq social care home
84.	Skemq social care home
85.	Strüna socialinês care home
86.	Stonaiéiq socialinés orphanage
87.	Special social care home "Tremtiniq namai"
88.	Social care home in Utena
89.	Veisiejq social care home
90.	Social care centre "Vija"
91.	Venta social care home
92.	Visaginas Social Care Home
93.	Zarasq social care home
94.	Algimantas Bandza Social Services Home

Efl. No.	Name of the legal entity
95.	Foster Home "Užuovėja"
Area of management of the Minister of Transport of the Republic of Lithuania	
96.	Ministry of Communications of the Republic of Lithuania
97.	Via Lietuva Joint Stock Company
98.	Lithuanian Transport Safety Administration
99.	Border Inspection Post Directorate under the Ministry of Transport and Communications
100.	Public institution "Plačiajuostis internetas"
Under the authority of the Minister for Health of the Republic of Lithuania	
101.	Ministry of Health of the Republic of Lithuania
102.	Hygienic Institute
103.	Kaunas Clinics of the Lithuanian University of Health Sciences Hospital
104.	National Public Health Laboratory
105.	National Transplantation Bureau under the Ministry of Health
106.	Centre for Radiation Protection
107.	Centre for Health Emergencies of the Ministry of Health
108.	State Forensic Medicine Laboratory
109.	State Forensic Psychiatry Unit under the Ministry of Health
110.	State Medicines Control Board under the Ministry of Health
111.	State Health Insurance Fund under the Ministry of Health
112.	Kaunas Territorial Health Insurance Fund
113.	Klaipėda Territorial Health Insurance Fund
114.	Panevezys Territorial Hospital Fund
115.	Šiauliai Territorial Health Insurance Fund
116.	Vilnius Territorial Hospital Fund
117.	Ambulance company
118.	Public institution Alytus County Tuberculosis Hospital
119.	Kaunas Hospital of Lithuanian University of Health Sciences
120.	Public body National Blood Centre
121.	Public institution Klaipėdos University Hospital
122.	Public body Klaipėda Republican Hospital
123.	Public institution Republican Hospital of Panevėys
124.	Public body Republican Hospital of Siauliq
125.	Public institution Vilnius Psychiatric Hospital
126.	Public institution Republican Vilnius University Psychiatric Hospital
127.	Public institution Rokiškis Psychiatric Hospital
128.	Public institution Vilnius Maternity Home
129.	Public body Vilnius University Hospital Santaros Klinikos
130.	National Public Health Centre under the Ministry of Health
131.	Republican Centre for Addictive Diseases
132.	State Accreditation Committee for Health Care Activities under the Ministry of Health
133.	Local institution Palangos vaíuj reabilitacijos sanatorija "Palangos gintaras"
Area of management of the Minister of Education, Science and Sport of the Republic of Lithuania	
134.	Ministry of Education, Science and Sport of the Republic of Lithuania
135.	National Education Agency
I3b.	National Institute of Science
Area of responsibility of the Minister of Justice of the Republic of Lithuania	
137.	Ministry of Justice of the Republic of Lithuania
138.	The Lithuanian Ministry of Justice
139.	Lithuanian Probation Service
140.	Lithuanian Centre for Forensic Sciences
141.	State Data Protection Inspectorate
142.	State Consumer Rights Protection Authority
143.	State Guaranteed Legal Aid Office
144.	State Patently Bureau of the Republic of Lithuania
Area of management of the Minister of Economy and Innovation of the Republic of Lithuania	
145.	Ministry of Economy and Innovation of the Republic of Lithuania
146.	Department of Standardisation of Lithuania
147.	National Digital Agenda Agency
148.	Lithuanian Metrology Inspectorate
149.	State Centre for State Registration of Information
150.	Public body CPO LT
Area of management of the Minister for Foreign Affairs of the Republic of Lithuania	
151.	Ministry of Foreign Affairs of the Republic of Lithuania (including diplomatic missions and consular offices of the Republic of Lithuania
Area of management of the Minister of the Interior of the Republic of Lithuania	
152.	Ministry of the Interior of the Republic of Lithuania

Efl. No.	**Name of the legal entity**
153.	Akcinć bcndrovć "Rcgitra"
154.	Personal Document and Registration Centre under the Ministry of the Interior
155.	Finansíniq nusikaltimq tyrirno tamyba under the Ministry of Internal Affairs
156.	Department of Informatics and Communications, Ministry of the Interior
157,	Medical Centre of the Ministry of the Interior
158.	Migration Department of the Ministry of the Interior
159.	Police Department under the Ministry of the Interior
160.	Alytus County High Police Commissariat
161.	Kaunas County Chief Police Commissariat
162.	Klaipėda County Chief Police Commissariat
163.	Lithuanian Criminal Police Bureau
164.	Lithuanian Police School
165.	Marijampolė County Chief Police Commissariat
166.	Panevezys County Chief Police Commissariat
167.	Šiauliai County Chief Police Commissariat
168.	Tauragė County Chief Police Commissariat
169.	Telśiq County Chief Police Commissariat
170.	Utena County Chief Police Commissariat
171.	Vilnius County Chief Police Commissariat
172.	Litekliq Agency under the Ministry of the Interior
173.	State Border Guard Agency under the Ministry of the Interior
174.	Public Security Agency under the Ministry of the Interior
175.	Department of Coastal Protection and Rescue under the Ministry of the Interior
176.	General Emergency Centre
177.	Fire Investigation Centre
178.	Fire and rescue hospital
	Area of responsibility of the Minister for Agriculture of the Republic of Lithuania
179.	Ministry of Agriculture of the Republic of Lithuania
180.	State Agricultural Data Centre
181.	National Inoculation Agency under the Ministry of Agriculture
182.	Fisheries Agency under the Ministry of Agriculture
183.	Land Agency under the Ministry of Agriculture
154.	State Crop Production Agency under the Ministry of Agriculture
185.	National Institute for Risk Assessment of Food and Vctcrinaria
186.	Office of the President of the Republic of Lithuania
187.	Chancellery of the Seimas of the Republic of Lithuania
188.	Seimas Ombudsmen's Office of the Republic of Lithuania
189.	Chancellery of the Government of the Republic of Lithuania
190.	Centre for Strategic Analysis of the Government
191.	The Government's representative body
192.	Department of State Security of the Republic of Lithuania
193.	Local Government Agency
194.	State Audit Office of the Republic of Lithuania
195.	Department of Drugs, Tobacco and Alcohol Control
196.	The Office of the Lithuanian Chief Archivist
197.	Kaunas Regional State Archive
198.	Klaipêda Regional State Archive
199.	Lithuanian Central State Archive
200.	Lithuanian Special Archive
201.	Lithuanian Literature and Art Archive
202.	Lithuanian State Historical Archive
203.	Lithuanian State New Archives
204.	Ğiauliq Regional State Archive
205.	Vilnius Regional State Archive
206.	Lithuanian Language Institute
207.	Prosecutor General's Office of the Republic of Lithuania
208.	National Judicial Administration
209.	National Court Administration Training Centre
210.	Bank of Lithuania
211.	State Food and Veterinary Office
212.	Local Purchasing Authority
213.	Central Electoral Commission of the Republic of Lithuania
214.	Communications Regulatory Authority of the Republic of Lithuania

Efl. No.	Name of the legal entity
215.	Special Investigation Agency of the Republic of Lithuania
216.	Management Protection Agency of the Republic of Lithuania
217.	Lithuanian Radio and Television Commission
218.	State Nuclear Energy Safety Inspectorate
219.	Chief Ethics Commission
220.	The Intelligence Ombudsperson's Office of the Republic of Lithuania
221.	Alytus District Court
222.	Kaunas Regional Court
223.	Kaunas District Court
224.	Klaipêda Regional Court
225.	Klaipêda District Court
226.	Marijampole District Court
227.	Panevèys Regional Court
228.	District Court of Panevezys
229.	Plungès District Court
230.	Ğiauliiț District Court
231.	Šiaulitț District Court
232.	Tauragês District Court
233.	Telšiai District Court
234.	Utena District Court
235.	Regîontț Administrative Court
236.	Vilnius Regional Court
237.	Vilnius City District Court
238.	Vilnius Regional District Court
239.	Court of Appeal of Lithuania
240.	Supreme Administrative Court of Lithuania
241.	Supreme Court of Lithuania
242.	Constitutional Court of the Republic of Lithuania
	Akmenès district municipality
243.	Akmenês district municipality administration
244.	Public bodyNaujosios Akmenês ligoninè-s zdrowatos centras
	Alytus City Municipality
245.	Alytus City Municipal Administration
246.	Public institution Alytaus apskrities S. Kudirkos ligoninê
247.	Public institution Alytus city municipality primary health care centre
248.	Public body Alytaus poliklinika
	Alytus district municipality
249.	Alytaus district municipality administration
250.	Alytaus rajono savivaldybês budgetinê ţstaiga Priešgaisñnés apsaugos tamyba
251.	Public institution Alytaus rajono savivaldybês primary health care centre
	Anykščiq District Municipality
252.	Anykščiiį rajono savivaldybês administration
253.	Public institution Anyksčiq district municipal hospital
254.	Public body Anykščilį district municipality primary health care centre
	Birštonas Municipality
255.	Birštonas Municipal Administration
256.	Public institution Birštonas Primary Health Care Centre
	Biržq District Municipality
257.	Biržtįtįon Municipal Administration
258.	Biržįon Municipal Fire Brigade
259.	Public institution Biržţţţ ligoninê
260.	Public institution Birźţţo rajono savivaldybês poliklinika
	Druskininkaiț Municipality
261.	Druskininluț Municipal Administration
262.	Public body Diuskininkq ligoninê
	Elektrènq municipality
263.	Elektrèniț Municipal Administration
264.	Fire-fighting and rescue services of the Municipality of Elektrènië
265.	Public Health Office of the Municipality of Elektrênq
266.	Public institution Abromiśkiiț Rehabilitation Hospital
267.	Public body Elektrënq 1hospital
268.	Public body Elektrêniț Municipal Health CenÕas
	Ignalina District Municipality
269.	Ignalina District Fire Brigade

Efl. No.	Name of legal entity
270.	lgnalina district municipal administration
271.	Public institution lgnalina district municipal health centre
	Jonava district municipality
272.	Jonava district municipality administration
273,	Public institution Jonava hospital
274.	Public institution Jonavos Pinninês Health Care Centre
	Joniskis District Municipality
275.	Administration of Joniskis district municipality
276.	Joniškis district municipality fire-fighting department
277.	Public institution Joniškis Hospital
	Jurbarkas district municipality
278.	Jurbarkas District Fire Brigade
279.	Administration of Jurbarkas district municipality
280.	Jurbarkas District Municipal Public Health Bureau
281.	Eržvilkas Primary Health Care Centre
282.	Public institution Jurbarkas Hospital
283.	Public institution Jurbarkas district primary health care centre
284.	Public institution Seredžiaus ambulatorija
285.	Public institution Šimkaičiq ambulatory
286.	Public body Vieivilés dispensary
	Kaišiadoriq district municipality
287.	Kaiiiadoriq district fire brigade
288.	Kaiiiadoriq district municipal administration
289.	Kaišiadoriq Primary Health Care Centre
	Kalvarija Municipality
290.	Kalvarija Fire and Rescue Service
291.	Kalvarija Municipal Administration
292.	Public institution Kalvarijos municipal health centre
	Kaunas City Municipality
293.	Kaunas city municipal administration
294.	Public institution K. Grinius nursing and palliative care hospital
295.	Via Kauno miesto poliklinika
	Kaunas district municipality
296.	Kaunas district municipality administration
297.	Public institution Garliavos Primary Health Care Centre
29ß.	Public institution Pakaunćs Primary Health Care Centre
299.	Public body Vilkija Primary Health Care Centre
	Kazlq Rüdos Municipality
300.	Administration of the Municipality of Kazlq Rüda
301.	Kazlq Rüda Municipality Fire Brigade
302.	Public body Kazlp Rüdos Pinninês Health Care Centre
	Kèdainiq District Municipality
303.	Kêdainiq District Municipal Administration
304.	Kêdainiq District Municipality Fire Brigade
305.	Local authority Kêdainiq hospital
306.	Public institution Kêdainiê Primary Health Care Centre
	Municipality of Kelmès
307.	Budgetary institution Kelmês District Priigaisrinés Safety Committee
308.	Kelmes District Municipal Administration
309.	Local authority Kelmês Hospital
310.	Public institution Tytuvėnq Primary Health Care Centre
311.	Public institution Kelmês District General Practitioner Centre
312.	Public institution Saukėnq dispensary
313.	Public body Kelmês District Primary Health Care Centre
	Klaipėda City Municipality
314.	Klaipeda City Municipal Administration
315.	Local institution Klaipêdos medicininês slaugos ligoninê
316.	Local institution Klaipėda vaiłu¡ hospital
317.	Local authority Klaipêdos city polyclinic
	Klaipėda District Municipality
318.	Klaipėda district municipal administration
319.	Klaipėda District Municipality Gargždas Hospital
320.	Klaipėda district municipality fire-fighting department
	Kretinga District Municipality
321.	Kretinga district municipality administration

Efl. No.	Name of legal entity
322.	Kretinga district municipality pricšgaisrinć tamyba
323.	Kretinga district municipality public institution Kartenos primary health care centre
324.	Kretinga district municipal public institution Kretingos ligoninć
325.	Kretinga district municipal public institution Kretinga primary health care centre
326.	Kretinga district municipal public institution Salantę primary health care centre
	Kupiskis District Municipality
327,	Kupiškis district municipal administration
328.	Access to the Kupiskis District Municipality
329.	Local authority Kupiikis ligoninê
330.	Public institution Kupiskis district municipality primary health care centre
	Lazdijtț District Municipality
331.	Lazdijtį district municipal administration
332.	Lazdijq district municipality
333.	Lazdijq local authority hospital
	Marijampolès Municipality
334.	Marijampolës municipal administration
335.	Local authority Marijampolês ligonińé
336.	Public institution Marijampolës Primary Health Care Centre
	Mažeikiq district municipality
337.	Mažeikiai district municipal administration
338.	Local authority Mažeikiq hospital
339.	Public institution Mažeikiq primary health care centre
340.	Public institution Seda Primary Health Care Centre
	Molèti¡ District Municipality
341.	Mo1ëtt¡ district municipal administration
342.	Public institution Molêttț District Health Centre
	Neringa Municipality
343.	Neringa Municipality Administration
344.	Public body Neringa Primary Health Care Centre
	Pagègiq Municipality
345.	Pagêgiq Municipal Administration
346.	Pagêgiq Municipal Council Access Control
347.	Public institution Pagêgiq Primary Health Care Centre
	Pakruojis District Municipality
348.	Pakruojis district municipality administration
349.	Local institution Pakruojo ligoninè
	Palanga City Municipality
350.	Administration of Palanga City Municipality
351.	Public institution Palanga Personal Health Care Centre
	Municipality of Panevezys City
352.	Administration of Panevêis City Municipality
353.	Public institution Panevêžio palliative treatment and nursing hospital
354.	Public institution Panevêžio miesto poliklinika
355.	Public body Panevêžio City Dental Clinic
35ò.	Public body Panevêžio Physical Medicine and Rehabilitation Centre
	Panevêžio District Municipality
357.	Administration of Panevêžio District Municipality
358.	Panevêžio rajono savivaldybês access control
359.	Public Health Bureau of Panevezys District Municipality
360.	Local institution Panevêžio rajono savivaldybês poliklinika
361.	Public institution Velžio komunalinis ükis
	Pasvalys District Municipality
362.	Pasvalys district municipal administration
363.	Pasvalys district municipality access control
364.	Public institution Pasvalys ligoninê
365.	Public institution Pasvalys Primary Health Care Centre
	Plungès district municipality
366.	Plungês district municipality administration
3fi7.	Plungês District Municipality Fire Protection Department
368.	Vicś%i istaiga Plungćs rajono savivaldybês ligoninê
	Prienq District Municipality
369.	Prieni¡ District Municipal Administration
370.	Prienij district municipality access control
371.	Local authority Prienq ligoninê

Efl.Nr.	Name of the legal entity
372.	Local institution Prienq district primary health care centre
373.	Radviliškis district municipal administration
374.	Public institution Radviliškis hospital
375.	Public institution Radviliškis district primary health care centre
376.	Public body Baisogala Primary Health Care Centre
377.	Public body Ğeduva Primary Health Care Centre
	Raseiniq district municipality
378.	Raseinitţ Fire Safety Committee
379.	Raseiniiţ District Municipal Administration
380.	Public institution Raseiniq ligoninê
381.	Public body Raseiniq Primary Health Care Centre
382.	Public institution Ariogala Primary Health Care Centre
	Rietavas Municipality
383.	Rietavas Municipal Administration
384.	Rietavas Municipality Fire Brigade
385.	Public institution Rietavas Primary Health Care Centre
	Rokiškis district municipality
386.	Rokiškis district municipality administration
387.	Rokiškis District Municipality Fire Brigade
388.	Public institution Rokiškio rajono ligoninë
389.	Public institution Rokiškis Primary Health Care Centre
	Šakiit District Municipality
390.	Šakiiţ district municipal administration
391.	Public Health Office of Šakiij District Municipality
392.	Public institution Kidulitţ dispensary
393.	Public institution Kudirkos Naumiescis Primary Health Care Centre
394.	Public institution Lekêčitţ ambulatory
395.	Public body Šakiiţ ligoninê
396.	Public body Šakitţ Primary Personal Health Care Centre
	Ğalčininkq district municipality
397.	Administration of Šalčininkai District Municipality
398.	Ğalčininktį district municipality fire brigade
399.	Local institution Šalčininktį Primary Health Care Centre
400.	Public institution Šalčinirikij district municipal hospital
	Šiauliai City Municipality
401.	Šiauliaiį city municipal administration
402.	Public institution Ğiauliij centro poliklinika
403.	Public institution Daínq Primary Health Care Centre
404.	Public institution Šiauliaiq long-term treatment and geriatric centre
405.	Public institution Šiauliq Rehabilitation Centre
406.	Šiauliaiţ City Municipal Public Health Bureau
	Šiauliai¡ District Municipality
407.	Šiauliaiţ District Municipal Administration
408.	Šiaulitţ District Municipality
409.	Public institution Šiauliai district municipal health centre
	Ğüalės District Municipality
410.	Šilalês District Municipal Administration
411.	Ğilalês district municipality fire brigade
412.	Public body Šilalės District Municipal Health Centre
413.	Public body Kaltinênij Primary Health Care Centre
	Municipality of Šüutês **District**
414.	Šilutês District Municipal Administration
415.	Fire brigade of Silutes district municipality
416.	Public institution Šilutės ligoninê
417.	Public institution Šilutês Primary Health Care Centre
	Širvinttţ District Municipality
418.	Širvinttţ District Municipal Administration
419.	Ğirvinttţ District Municipality
420.	Public institution Širvintiţ District Municipal Health Centre
	Skuodas District Municipality
421.	Skuodas district municipal administration
422.	Skuodas district municipality fire brigade
423.	Skuodas Primary Health Care Centre

Efl.Nr.	Name of legal entity
424.	Public institution Mosêdžio Primary Health Care Centre
	Švenćioniq District Municipality
425.	Fire protection service at the administration of Švenčioniq district municipality
426.	Ǧvenčioniq District Municipal Administration
427.	Public body ǦvenǦioniiį District Health Centre
	Tauragès District Municipality
428.	Tauragês district municipal administration
429.	Fire brigade of Tauragês district municipality
430.	Public institution Tauragés ligoninè
431.	Public institution Tauragês district primary health care centre
	Telsiq district municipality
432.	Telàitįyonas Municipal Administration
433.	Telšiq District Municipality
434.	Public institution Regional Teliiq Hospital
435.	Te1šiį District Primary Health Care Centre
	Trakq District Municipality
436.	Traktįrajon fire-fighting and rescue agency
437.	Trakq district municipal administration
438.	Public institution Onuškio palliative treatment and nursing hospital
439.	Public institution Trakiț ligoninê
440.	Public institution Lentvario arribulatorija
441.	Public body Trakq Primary Health Care Centre
	Ukmergès district municipality
442.	Ukmergês district municipal administration
443.	Ukmergés district municipality fire brigade
444.	Public institution Ukmergês ligoninê
445.	Public institution Ukmergés Primary Health Care Centre
	Utenos rajono savivaldybè
446.	Administration of Utena district municipality
447.	Fire brigade of Utena district municipality
448.	Public Health Bureau of Utena District Municipality
449.	Public institution Utena hospital
450.	Public body Utena Primary Health Care Centre
451.	Public body St. Clara palliative care and nursing hospital
	Varëna District Municipality
452.	Varèna District Municipality Administration
453.	Varenna District Municipality's Access Protection Department
454.	Public institution Varèna Health Centre
	Vilkaviškis district municipality
455.	Biudgetinê jstaiga VÎlkaviikio rajono priešgaisrinê tamyba
456.	Public institution Vilkaviškis ligoninê
457.	Public body Vilkaviikio Primary Health Care Centre
458.	Vilkaviikio rajono savivaldybès administracija
	Vilnius City Municipality
459.	Public institution Antakalnis poliklinika
460.	Public institution Centro poliklinika
461.	Public institution Grigiskitț health care cenÕas
462.	Public ţinstitutionNaujosios Vĺnios poliklinika
463.	Public ţinstitution Karoliniškiiț polyclinic
464.	Public institution Šeškìnês polyclinic
465.	Public institution Vilnius City Mental Health Centre
466.	Public institution Mykolas Marcinkevicius Hospital
467.	Public institution St. Roko Hospital
468.	Public institution Vilkpëdės 1hospital
469.	Public institution Vilnius City Clinical Hospital
470.	Vilnius City Municipality Administration
471.	Vilnius City Municipality Public Health Bureau
472.	Public institution Vilniaus rajono Nemenčinés poliklinika
	Vilnius District Municipality
473.	Vilnius District Municipal Administration
474.	Vilnius district municipality fire-fighting department
475.	Public institution Vilniaus rajono centrinê poliklinika
	Visaginas Municipality
476.	Public institution Visagino ligoninê

Efl.Nr.	Name of legal entity
477.	Visaginas Municipality Administration
	Zarasq district municipality
478.	Zarasi¡ fire protection organisation
479.	Zarasit district municipal administration
480.	Zarasq district municipal public institution Health Centre

APPROVED
The Government of the Republic of Lithuania
Resolution No. 818 of 13 August 2018 (Government
of the Republic of Lithuania
Resolution No. 945 of the Republic of Lithuania of
6 November 2024)

DESCRIPTION OF THE CRITERIA FOR DETERMINING THE REFUND FOR THE USE OF ADDITIONAL ELECTRONIC COMMUNICATIONS AND Cybersecurity SERVICES PROVIDED THROUGHOUT THE SECURE STATE DATA TRANSMISSION NETWORK AND THE PROCEDURE FOR THE CALCULATION OF THE REFUND

CHAPTER I GENERAL PROVISIONS

1. The criteria for determining the amount of remuneration for the use of additional electronic communications and cyber s e c u r i t y services provided over the Secure State Data Communications Network and the procedure for calculating the remuneration (hereinafter referred to as 'the Regulations') shall lay down the criteria for determining the amount of remuneration for the use of The Regulation establishes the criteria for determining the amount of additional electronic communications and cybersecurity services (hereinafter referred to as "additional services") (hereinafter referred to as "remuneration levels") provided by the Secure State Data Transmission Network (hereinafter referred to as "remuneration levels") and the calculation of the remuneration levels, the procedure for the calculation, adjustment and approval of the remuneration.

2. The terms used in the Description shall be understood as defined in the Law on Cyber Security of the Republic of Lithuania, the Law on Electronic Communications of the Republic of Lithuania.

CHAPTER II
CRITERIA FOR DETERMINING THE REMUNERATION AND CALCULATION OF THE REMUNERATION

3. The manager of the secure network shall calculate the remuneration levels by the end of the calendar year in accordance with the criteria for determining the remuneration levels referred to in point 4 of the Regulation.

4. Criteria for determining remuneration:

4.1. the cost of the ancillary service (iilaidos), based on the material and equivalent costs (depreciation of tangible fixed assets and amortisation of intangible fixed assets) of the Safety Net Manager providing the ancillary service in the previous calendar year, utilities, electronic communications services, repairs, maintenance of the electronic communications network) and labour costs (wages, social security charges) incurred in the provision of the specific additional service;

4.2. the cost (iilaidos) of the supplementary service to be provided, based on the estimated costs referred to in point 4.1 of the Annex.

5. Only costs directly related to the provision of the ancillary service may be included in the calculation of the remuneration.

6. The safety net manager shall enter into an agreement with an auditor or audit firm, as defined in the Law on auditing and other assurance services of the Republic of Lithuania (hereinafter referred to as 'audit firm'), for an additional service to the cost of providing the service (hereinafter referred to as 'audit').

7. The safety net manager, after calculating the remuneration, shall provide the audit body with all the detailed information justifying the costs of providing the additional service and any other information relevant for verifying the costs of providing the additional service, no later than 1 month after the end of the calendar year.

8. The audit body shall have the right to obtain from the Safety Net Manager additional data and explanations necessary to verify the cost of providing the additional service.

9. After the audit team has carried out an inspection and submitted an inspection report indicating the calculation of the additional costs for the provision of the service, the SecurityNetwork Manager shall be obliged to resolve the shortcomings indicated by the audit team. In the case referred to in this point, an additional audit report shall be obtained.

10. If the audit body has carried out an inspection and has not found any deficiencies in the calculation of the costs of the provision of the additional service, the Safety Net Manager shall submit the information on the calculated remuneration and the verified data on the costs incurred to the body authorised by the Government of the Republic of Lithuania within the time limit referred to in Article 37(8) of the Law on Cybersecurity.

11. The authority received by the government shall not start the preparation of the report until all the information necessary for the conclusion has been received. The body empowered by the Government shall, within 15 working days of receipt of all the information necessary for the opinion, give an opinion on whether the remuneration levels have been calculated taking into account the criteria for determining the remuneration levels referred to in point 4 of the Regulation. If the competent authority of Vyriausybės finds that the remuneration rates have not been calculated taking into account the criteria referred to in point 4 of the Regulation, it shall inform the operator of the safety net, which shall, within a period of no more than 10 working days from the receipt of such information, rectify the identified shortcomings and resubmit the verified data on the costs incurred and remuneration rates.

12. The manager of the safety net, having received a conclusion of the body authorised by the Government that the remuneration rates have been calculated taking into account the criteria for determining the remuneration rates referred to in point 4 of the Description, shall submit the calculated remuneration rates and all related information to the Minister of National Defence within 10 working days from the date of receipt of the conclusion.

13. The salary levels shall be recalculated annually. Approved salary scales shall be amended only if they differ from the newly calculated salary scales. The newly calculated rates must be approved at the latest within 3 months after the end of the calendar year.

CHAPTER III FINAL PROVISIONS

14. The remuneration rates, the inspection reports and the conclusions of the Governmental Authority shall be made publicly available on the website of the Safety Net Manager.