Consolidated version from 01-01-2019

Resolution published:TAR 2018-08-21, i. k. 2018-13252

THE GOVERNMENT OF THE REPUBLIC OF LITHUANIA

RESOLUTION
ON THE IMPLEMENTATION OF THE LAW OF THE REPUBLIC OF LITHUANIA ON CYBER SECURITY

13 August 2018 No. 818
Vilnius

Legislative title changed:
No. 1209, 2018-12-05, published TAR 2018-12-10, i. k. 2018-20153

In accordance with Article 5(1-5) of the Law of the Republic of Lithuania on Cyber Security, and through the implementation of the Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 on concerning measures for a high common level of security of network and information systems across the Union (*OJ L 194, 19.7.2016, p. 1–30*), the Government of the Republic of Lithuania decides to:

Preamble changes:

No. 1209, 2018-12-05, published TAR 2018-12-10, i. k. 2018-20153

1. Approve the attached:

1.1. National Cyber Security Strategy;

1.2. Identification Methodology for Critical Information Infrastructure (hereinafter referred to as "Methodology");

1.3. Description of the organizational and technical cyber security requirements applicable to cyber security entities (hereinafter referred to as “Description”);

1.4. National Cyber Incident Management Plan (hereinafter referred to as the “Plan”).

Amendments:

No. 1209, 2018-12-05, published TAR 2018-12-10, i. k. 2018-20153

2. Confer on the Ministry of National Defense of the Republic of Lithuania to submit a draft Interinstitutional Action Plan for the Implementation of the National Cyber Security Strategy to the Government of the Republic of Lithuania for approval before 2 November 2018;

3. Suggest:

3.1. non-governmental organizations, public and private sector stakeholders, Lithuanian research and academic institutions to participate in the implementation of the National Cyber Security Strategy;

3.2. Chancellery of the Office of the President of the Republic of Lithuania, the Chancellery of the Parliament of the Republic of Lithuania, the Central Electoral Commission of the Republic of Lithuania, the Office of the Chief Archivist of Lithuania shall, under the procedure laid down in Methodology, identify all the infrastructures in their field of activity, which are important in the provision of critical services within the general government sector, complete a questionnaire included in Annex 2 of the Methodology, submit it to the authority or authorities referred to in Annex 1 of the Methodology and perform the functions of Responsible Manager under the procedure laid down in Methodology;

3.3. The Prosecutor General's Office of the Republic of Lithuania, the National Courts Administration, the Special Investigation Service of the Republic of Lithuania shall, in accordance with the procedure laid down in the Methodology, identify all the infrastructures in their field of activity, which are important in the provision of critical services within general government sectors, as well as within the sectors of public security and rule of law, complete a questionnaire included in Annex 2 of the Methodolog, submit it to the authority or authorities referred to in Annex 1 of the Methodology, and perform the functions of the Responsible Manager under the procedure laid down in Methodology;

3.4. The Communications Regulatory Authority of the Republic of Lithuania to cooperate, in the area of its competence, with the Ministry of Transport and Communications of the Republic of Lithuania, and to provide the necessary expert assistance in performing the functions, as laid down in Methodology, of the Responsible Authority in the digital communications sub-sector of the information technology and digital communications sector;

3.5. To the municipal authorities of the Republic of Lithuania, under the procedure laid down in the Methodology, to identify all infrastructures in their field of activity, which are important in the provision of critical services in energy, transport and postal, health care, drinking water supply, distribution and management, general government sectors, complete a questionnaire included in Annex 2 of the Methodology, submit it to the authority or authorities rerferred to in Annex 1 of the Methodology, and perform the functions of the Responsible Manager under the procedure laid down in Methodology;

3.6. The Bank of Lithuania, in accordance with the Point 2(3), to designate the responsible people to perform the functions, under the procedure laid down in this Resolution and Methodology, of bodies in the finance sector, as defined in Annex 1 in Methodology,

3.7 authroties, as listed in Point 5 of Plan, except the Ministy of National Defense of the Republic of Lithuania, to designate people responsible for the transmission of information, in accordance with the procedure laid down in the Plan, and to provide their contact details to the National Cyber Security Centre under the Ministry of National Defence.

Amendments:

No. 1209, 2018-12-05, published TAR 2018-12-10, i. k. 2018-20153

4. Assign:

4.1. the authorities, referred to in Annex 1 to the Methodology, until February 1, 2019, to initiate, under the procedure laid down in Methodology, the review of critical infrastructure and refer to the institutions, bodies, enterprises or their departments, which are a part of critical infrastructure, or to the infrastructure manager (hereinafter referred to as "Responsible manager"), when a part of a infrastructure is a device or a part of a device, asking Responsible managers to assess the significane of the entire managed infrastructure, and complete the questionnaire included in Annex 2 to the Methodology;

4.2. the authorities, referred to in Annex 1 to the Methodology, until February 1, 2019, to designate people responsible establishing a list of critical infrastructure operating within the sectors of critical importance and provisioning critical services, and a list of critical information infrastructures, and to provide their contact details to the Ministry of National Defence;

4.3. The Ministry of National Defence, until 2019 February 1, to designate people responsible for transmitting information, in accordance with the procedure laid down in the Plan, and to provide their contact details to the National Cyber Security Centre;

4.4. the authorities, referred to in Point 4 of the Plan, until February 1, 2019, to designate people, who are available around the clock, and are responsible for exchanging information during a cyber incident management process, to establish rules of how and when can they be substituted, and to confer on the State Data Protection Inspectorate and the Police Department with providing their contact details to the National Cyber Security Centre;

4.5. cyber security entities, by 2019 February 1, to appoint responsible people available around the clock, and provide their phone numbers, e-mail addresses, and other contact details enabling the exchange of information around the clocek, to the National Cyber Security Centre.

Added point:

No. 1209, 2018-12-05, published TAR 2018-12-10, i. k. 2018-20153

Prime Minister Saulius Skvernelis

Minister of National Defence Raimundas Karoblis

APPROVED by
decree No. 1209 of the Government of the
Republic of Lithuania of 5 December 2018

DESCRIPTION OF THE ORGANIZATIONAL AND TECHNICAL CYBER SECURITY REQUIREMENTS APPLICABLE TO CYBER SECURITY ENTITIES

CHAPTER I
GENERAL PROVISIONS

1. The description of the organizational and technical cyber security requirements for cyber security entities (hereinafter referred to as "Description") sets out the organizational and technical cyber security requirements (collectively referred to as "Requirements") for cyber security entities.

2. The terms used in the Description are defined in the Law of the Republic of Lithuania on Cyber Security, the Law on the Management of State Information Resources of the Republic of Lithuania, the Law on Electronic Communications of the Republic of Lithuania, the Law on State and Service Secrets of the Republic of Lithuania and the General Requirements for Electronic Information Security approved by the Government of the Republic of Lithuania in 2013 July 24 by Decree No. 716 "Description of General requirements on electronic information security, of the Description of guidelines on the content of security documents and the Description of guidelines on the classification of state information systems, registers and other information systems and determination of importance of electronic information.“

CHAPTER II
RISK ASSESSMENT OF COMMUNICATION AND INFORMATION SYSTEMS OF CYBER SECURITY ENTITIES

3. The provision of cyber security organizational and technical measures for cyber security communications and information systems shall be based on a risk assessment of threats and vulnerabilities that may affect cyber security for communications and information systems, taking into account the latest technical developments. Cyber security entities organizing risk assessment of communication and information systems shall:

3.1 designate a person or persons responsible for risk assessment, monitoring and continuous improvement of the risk assessment process and determine the qualification requirements applicable to them. The responsible person may be an employee of a cyber entity or a contract may be concluded with an entity providing the services of risk assessment, monitoring and continuous improvement of the risk assessment process;

3.2. set requirements for the risk assessment process, risk prioritization criteria and acceptable risk level;

3.3. identify threats and vulnerabilities that may affect cyber security for communications and information systems, and identify potential threat and vulnerability areas that may affect their ongoing activities;

3.4. assess the likelihood and consequences of threats for communication and information systems, determine their level of risk, assess likelihood of identified threats and prioritize them in order of importance, which is based on a performed risk assessment ;

3.5. in accordance with the procedure set out in the Description and based on a performed risk assessment, prepare and / or review the approved legal acts regulating state information resources or critical information infrastructure cyber security policy and its implementation (hereinafter referred to as "cyber security policy and its implementation documents"); and / or cyber security rules for the providers of public communications networks and/or public digital communication services and other digital services, and determine which of their cyber security requirements need to be updated and / or implemented first to ensure cyber security of communication and information systems.

4. When organizing risk assessment of communication and information systems, it is recommended to follow Lithuanian and international standards or methodologies regulating risk management processes and to include risk assessment of communication and information systems in the overall risk assessment processess of cyber security entities.

CHAPTER III
ORGANIZATIONAL CYBER SECURITY REQUIREMENTS APPLICABLE FOR ENITITIES CONTROLING AND / OR MANAGING STATE INFORMATION RESOURCES AND MANAGERS OF THE CRITICAL INFORMATION INFRASTRUCTURE

5. Entities controling and / or managing state information resources and managers of the critical information infrastructure shall:

5.1. at least once a year or after major organizational or systemic changes, organize and conduct a risk assessment in accordance with the procedure set out in Chapter II of the Description. Entities controling and / or managing state information resources and managers of the critical information infrastructure shall have the right to conduct a risk assessment in conjunction with the state information resources or critical information infrastructure risk assessment and / or information technology security conformity assessment;

5.2. taking into account the results of the performed risk assessment, as well as deficiencies identified in the management and elimination of cyber incidents, and in business continuity management efforts, improve the business continuity management plans of the state information resources and cyber incident response plans for the critical information infrastructure. The results of the effectviveness test of the business continuity management plans or cyber incident response plans for the critical information infrastructure shall be set out in the their tested effectiveness and observed deficiencies report. Copies of these reports shall be submitted to the National Cyber Security Center no later than five working days after the adoption of these documents;

5.3. approve the cyber security policy and its implementation documents in agreement with the National Cyber Security Center, which must set out:

5.3.1. all applications and uses of cyber security policy and its implementation documents;

5.3.2. the formation of the state information resources and critical information infrastructure user groups, the provision and management of rights and access to state information resources or critical information infrastructure services and resources;

5.3.3. cyber security-related duties and functions of the state's information resources and critical information infrastructure users;

5.3.4. cyber security training for state‘s information resources and critical information infrastructure user, or other competent person or department responsible for the organization and provision of cyber security measures;

5.3.5. the procedure for creating, securing and changing usernames and passwords for state information resources or critical information infrastructure users;

5.3.6. the procedure for administrating and storing audit logs;

5.3.7. the procedure for the detection and prevention of cyber intrusions;

5.3.8. the rules for a secure use of wireless networks;

5.3.9. the rules for a secure use and control of mobile devices used to access state information resources or critical information infrastructure;

5.3.10. data encryption settings on mobile devices;

5.3.11. the use of state information resources or critical information infrastructure resources outside the organization and / or mobile devices;

5.3.12. security management of websites used by the state‘s information resources or critical information infrastructure;

5.3.13. the procedure for assesssing cyber threats and vulnerabilities that may affect the state information resources or critical information infrastructure;

5.3.14. the rights and obligations of the entities involved in vulnerability assessment process;

5.3.15. the preparation a vulnerability assessment plan;

5.3.16. the use of a vulnerability detection software;

5.3.17. the classification of vulnerability assessment results;

5.3.18. the preparation of vulnerability assessment reports and addressing identified security gaps;

5.3.19. the organization of a cyber incident response plan;

5.3.20. the processess for cyber incident detection;

5.3.21. the procedure for cyber incident assessment;

5.3.22. the procedure for handling and eliminating cyber incidents;

5.3.23. the procedure for restoring state's information resources or critical information infrastructure‘s normal activity and defining the maximum permissible time period for service‘s inactivity;

5.3.24. the procedure for the assessment of acquired cyber incident management experience;

5.3.25. the procedure for installing and configuring cyber security solutions;

5.3.26. the procedure for the implemention control and conformity assessment of Requirements;

5.3.27. the procedure for improving the cyber security level of the state information resources or critical information infrastructure;

5.3.28. the use of email.

6. Entities managing and / or managing state information resourcesshall have the right to set out the information or documents, laid down in Sub-paragraph 5.3 of the Description, in the prepared and adopted safety documentation in accordance with the General Electronic Information Security Requirements. Mentioned safety documents shall be further aligned in accordance with the procedures established in the General Requirements for Electronic Information Security.

7. The National Cyber Security Center shall submit conclusions, comments and suggestions for cyber security policy drafts and their policy implementation documents within ten working days, if these projects are large (more than ten pages) - within fifteen working days, and re-submitted draft documents - within five working days of receipt. Before submitting conclusions, comments, and suggestions for the cyber security policy drafts and their implementation documents, the National Cyber Security Center has the right to request the managers of state information resources or critical information infrastructure to provide

supporting documents approving the security of the state information resources or critical information infrastructure.

8. The cyber security policy and its implementation documents shall be reviewed (revised) at least once a year. Changes to the cyber security policy and its implementation documents may be excluded from coordinating with the National Cyber Security Center in cases when only editorial amendments are being made. In such cases, copies of these documents shall be provided to the National Cyber Security Center.

9. The Requirements conformity assessment of the state information resources or critical information infrastructure shall be organized and carried out at least once a year.

10. The analysis of the state information resources or critical information infrastructure and state information resources or critical information infrastructure users audit logs shall be performed at least once a month.

11. The analysis of the occurrences recorded by the firewall and the elimination of any observed non-conformity cases with the security requirements shall be carried out at least once month.

12. Software and patch updates for cyber security measures shall be updated and installed at least once a month.

13. Prior to conducting tender procedure, in the contract documents, state information resources managers, managers of the critical information infrastructure intending to purchase services, works or equipment related to state information resources or critical information infrastructure and its design, development, implementation, modernization and cyber security must ensure that the service provider, contractor or equipment provider ensures conformity with the Requirements.

CHAPTER IV
TECHNICAL CYBER SECURITY REQUIREMENTS APPLICABLE FOR THE ENITITIES CONTROLING AND / OR MANAGING STATE INFORMATION RESOURCES AND MANAGERS OF THE CRITICAL INFORMATION INFRASTRUCTURE

14. The technical cyber security requirements for the entities controlling or managing state information resources and managers of the critical information infrastructure shall be determined according to the importance of the state information resources or critical information infrastructure, as follows:

14.1. Critical Information Infrastructure (CII);

14.2. first category (I);

14.3. second category (II);

14.4. third category (III);

14.5. fourth category (IV).

15. The categories of importance of the state information resources shall be determined in accordance with the Description of guidelines on the classification of state information systems, registers and other information systems and determination of importance of electronic information, approved by Resolution No 716 of the Government of the Republic of Lithuania of 24 July 2013 on the approval of the Description of general requirements on electronic information security, of the Description of guidelines on the content of security documents and the Description of guidelines on the classification of state information systems, registers and other information systems and determination of importance of electronic information.

16. A detailed list of technical cyber security requirements is provided in the Annex to the Description.

17. The cyber security measures specified in the Annex shall be implemented in accordance with the state of the art technological developments and in accordance with at least one good security practice recommendation provided by its manufacturer.

CHAPTER V
REQUIREMENTS FOR SERVICE PROVIDERS OF PUBLIC COMMUNICATIONS NETWORKS AND/OR PUBLIC DIGITAL COMMUNICATION SERVICES

18. Providers of public communications networks and / or public digital communications services:

18.1. at least once every two years or after major organizational or systemic changes, organize and perform risk assessment in accordance with the procedure set out in Chapter II of the Description. The risk assessment shall be carried out by the providers of public communications networks and / or public digital communications services in conjunction with the conformity assessment of operational risk and / or information technology security;

18.2. implements organizational and technical measures to ensure that the flow of counterfeit Internet Protocol (IP) addresses is blocked on their public communications networks;

18.3. implements organizational and technical measures to ensure that the denial of service (DoS) attacks are blocked on their public communications networks;

18.4. implements organizational and technical measures to ensure the cyber security of systems and equipment used for their public communications networks and / or public digital communications services;

18.5. maintains and updates its cyber security management rules for public communications networks and / or public digital services, following major organizational or systemic changes, and submits them to the National Cyber Security Center at the request of the National Cyber Security Center. The rules for cyber security management of public communications networks and / or public digital services shall specify:

18.5.1. descriptionsof measures required to manage cyber incidents;

18.5.2. the plan for ensuring the continuous provision of public communications networks and / or public digital communications services and the conditions for its application and the maximum permissible time period for service‘s inactivity;

18.5.3. the duties and responsibilities of those responsible for the management of cyber incidents;

18.5.4. the procedures and conditions for the monitoring, verification, testing and auditing of systems and equipment used for the provision of public communications networks and / or public digital communications services;

18.5.5. compliance with Lithuanian and international standards describing cyber security or secure digital information management;

18.6. inform the recipients of public digital communications services, free of charge, on the means, which the recipients of public digital communications services may, in cases of a cyber incident threat needs to be eliminated, related to the use of endpoint devices of the recipients of public digital communications services, and indicate the likely costs of such use;

18.7. inform the recipients of the public digital communications services and the National Cyber Security Center not later than five working days about the planned and scheduled work, which is likely to impair the cyber security of public communications networks and / or public digital communications services;

18.8. make publicly available recommendations to users of public digital communications services on cyber security measures through the use of public communications networks and / or providers of public digital communications services.

CHAPTER VI
REQUIREMENTS FOR DIGITAL INFORMATION HOSTING SERVICE PROVIDERS AND DIGITAL SERVICE PROVIDERS

19. Digital information hosting service providers and digital service providers:

19.1. at least once every two years or after major organizational or systemic changes, organize and perform risk assessment in accordance with the procedure set out in Chapter II of the Description. Digital information hosting service providers and digital service providers have the right to carry out the risk assessment together with operational risk and / or information technology security conformity assessment;

19.2. together with the providers of public communications networks and / or public digital communications services, take appropriate measures to ensure cyber security;

19.3. implement organizational and technical measures to ensure the cyber security of their systems and devices used for digital information hosting or digital services;

19.4. maintain and update their cyber security management rules after major organizational or systemic changes, and submit them to the National Cyber Security Center at the request of the National Cyber Security Center. Cyber security management rules for digital information hosting service providers and digital service providers should include the following:

19.4.1. description of required measures to manage cyber incidents;

19.4.2. a plan for ensuring the continuous provision of digital information hosting service providers and digital service providers, and the conditions for its application and the maximum permissible time period for service‘s inactivity;

19.4.3. the duties and responsibilities of those responsible for the management of cyber incidents;

19.4.4. the procedures and conditions for the monitoring, verification, testing and auditing of systems and equipment used for the provision of public communications networks and / or public digital communications services;

19.4.5. compliance with Lithuanian and international standards describing cyber security or secure digital information management;

19.5. inform free of charge the beneficiaries of the digital information hosting and digital services about any identified cyber incidents related to digital information hosting or digital services, which are attributed as having high potential impact, as identified in the National Cyber Incident Management Plan;

19.6. inform the beneficiaries of the digital information hosting and digital services and the National Cyber Security Center not later than five working days about the planned and scheduled work, which may impair the cyber security of digital information hosting and digital services;

19.7. inform the beneficiaries of the digital information hosting and digital services about the countries where their digital information, which is created, managed or provided for storage using digital information hosting and digital services, may be hosted, and specify in which cases such information may be transferred to other countries;

19.8. establish a warning system to inform the beneficiaries of the digital information hosting and digital services about the cyber security breaches of digital information hosting and digital services, and what action must be taken by digital information hosting service and digital service beneficeries and / or providers;

19.9. make publicly available recommendations to the beneficiaries of the digital information hosting and digital services about the means to ensure cyber security when using digital information hosting or digital services.

CHAPTER VII
FINAL PROVISIONS

20. Cyber security entities have the right to define and apply additional Requirements. If the additional Requirements establish the technical and organizational cyber security measures are equivalent, and include the Requirements set out in the Description, cyber security entities have the right to apply only additional Requirements.

21. Cyber security entities, with the exception of digital service providers, shall provide the National Cyber Security Center with the technical information necessary to assess the cyber security of their communication and information systems. Information shall be provided:

21.1. at the request of the National Cyber Security Center on the basis of format and terms specified by it;

21.2. on the initiative of the cyber security entities.

22. The National Cyber Security Center shall have the right to process cyber security information, provided by cyber security entities, including confidential information, only to the extent necessary to assess the cyber security of communication and information systems managed by cyber security entities.

23. It is recommended that the implementation of technical cyber security measures by service providers of public communications networks and/or public digital communication services, providers of digital information hosting services and providers of digital services by following the list of technical cyber security requirements listed the Annex to the Description.

_____

Description of organizational and
technical cyber security requirements for
cyber security entities
Annex

LIST OF TECHNICAL CYBER SECURITY REQUIREMENTS APPLICABLE TO ENITITIES CONTROLING AND / OR MANAGING STATE INFORMATION RESOURCES AND MANAGERS OF THE CRITICAL INFORMATION INFRASTRUCTURE

Table 1. Digital identification, confirmation of identity and security and control measures of the use of state information resources or critical information infrastructure

Requirement	Category by importance				
	Critical Information Infrastructure (CII)	**I**	**II**	**III**	**IV**
1. The functions of a person responsible for maintaining state information resources or critical information infrastructure (hereinafter referred to as "Administrator") shall be performed using a separate dedicated account that may not be used to perform the regular user tasks with state information resources or critical information infrastructure .	x	x	x	x	x
2. User of state information resources or critical information infrastructure should not be granted with administrator-level privileges	x	x	x	x	x
3. Each user of state information resources or critical information infrastructure must be uniquely identifiable (the identity number cannot be used to identify the user of state information resources or critical information infrastructure)	x	x	x	x	x
4. The confidentiality of information transmitted over public digital communications networks must be secured by encryption, a virtual private network (VPN)	x	x	x	x	x
5. The user or administrator of the state information resources or critical information infrastructure must authenticate its identity with a password or other means of authentication	x	x	x	x	x
6. Two-factor authentication measures must be used to authenticate administrators (if state information resources or critical information infrastructure parts support such functionality)	x	x	x		
7. The right of a user of state information resources or critical information infrastructure to work with a particular state information resource or critical information infrastructure shall be suspended when a user of state information resources or critical information infrastructure does not use state information resources or critical information infrastructure longer than three months (if parts of the state information resources or critical information infrastructure support such functionality).	x	x	x	x	x

8. The Administrator's right to work with the state information resources or critical information infrastructure must be suspended when the Administrator does not use the state information resources or critical information infrastructure longer than two months (if parts of the state information resources or critical information infrastructure support such functionality)	x	x	x	x	x
9. In cases prescribed by law, a user or administrator of a state information resources or critical information infrastructure is removed from work (duties), does not meet the state information resources or critical information infrastructure user or administrator qualification requirements specified in other legal acts, his / her work (service) shall also be terminated, he / she loses credibility, right of access to state information resources or critical information infrastructure must be revoked immediately	x	x	x	x	x
10. Unnecessary or unused users and administrator accounts to connect to state information resources or critical information infrastructure must be blocked immediately and deleted after the audit term storage term expires.	x	x	x	x	x
11. When work is completed or a user of a state information resources or critical information infrastructure leaves its workplace, steps must be taken to prevent unauthorized access to information handled by state information resources or critical information infrastructures: worksations with the access to state information resources or critical information infrastructure, must be logged off and locked with a password-enabled screensaver (if parts of the state information resources or critical information infrastructure support such functionality)	x	x	x	x	x
12. In the absence of any action taken by the user of state information resources or critical information infrastructure, the workstation shall be locked in order to continue to enable the access to state information resources or critical information infrastructure only after repeatedly authetincating users‘s identity (if parts of the state's information resources or critical information infrastructure support such functionality). The time after which, in the absence of any action, state information resources or critical information user‘s workstation is locked shall be set out in the cyber security policy and its implementation documents, but it may not exceed fifteen minutes. This requirement does not apply if following the risk assessment of the communication and information systems, other cyber security measures are taken, which correspond to the previously identified risks.	x	x	x	x	x
13. Passwords requirements for accessing state information resources or critical information infrastructure:					
13.1. The password must consist of letters, numbers and special characters	x	x	x	x	x
13.2. Personal information (such as date of birth, family names, etc.) should not be used to generate passwords	x	x	x	x	x
13.3. It is forbidden to disclose passwords to others	x	x	x	x	x
13.4. Parts of the state information resources or critical information infrastructure authenticating the identity the user of state information resources or critical information infrastructure	x	x	x	x	x

shall prohibit saving passwords (if parts of the state information resources or critical information infrastructure support such functionality).					
13.5. The maximum permissible number of attempts (up to five) to enter the correct password by the user of state information resources or critical information infrastructure should be established (if parts of state information resources or critical information infrastructure support such functionality). If user's attempts to type its password reaches the established number of attempts, user account must be locked and user shall be prevented from accessing the state information resources or critical information infrastructure for a minimum of fifteen minutes as established in state information resources or critical information infrastructure cyber security policy and its implementation documents (if parts of state information resources or critical information infrastructure support such functionality)			x	x	x
13.6. The number of attempts by the user of state information resources or critical information infrastructure to enter the correct password shall be limited to three times (if parts of the state information resources or critical information infrastructure support such functionality). If user enters the password incorrectly as many times as it has been limited to, the state information resources or critical information infrastructure user account must be blocked and the administrator must be notified about it (if parts of the state information resources or critical information infrastructure support such functionality)	x	x			
13.7. Passwords cannot be stored or transmitted in open text. In the decision of a competent person or departament responsible for the organization and security of cyber security, only a temporary password may be transmitted in open text, but separately from the username, if the user of the state information resources or critical information infrastructure has no possibility to decipher the encrypted password received, or if there is no technical capability to send the password to the user of state information resources or critical information infrastructure through an encrypted channel or a secure digital communications network	x	x	x	x	x
13.8. Additional passwords requirements for state information resources or critical information infrastructure users:					
13.8.1. The password must be changed at least once every three months	x	x	x	x	
13.8.2. The password must be at least eight characters long (if parts of the state information resources or critical information infrastructure support such functionality)	x	x	x	x	
13.8.3. When the password is being changed, state information resources or critical information infrastructures must not allow the password to be generated from the previous six used passwords (if parts of the state information resources or critical information infrastructure support such functionality)	x	x	x		
13.8.4. When the user connects to a state information resource or critical information infrastructure for the first time, it must be required to change the default password for accessing the state information resources or critical information infrastructure (if parts	x	x	x	x	x

of the state information resources or critical information infrastructure support this functionality)					
13.9. Additional password requirements for administrators:					
13.9.1. The password must be changed at least once every two months	x	x	x	x	
13.9.2. The password must be at least twelve characters long (if the state information resources or critical information infrastructure parts support such functionality)	x	x	x	x	
13.9.3. When the password is being changed, the application software must not allow the password to be generated from the previous three used passwords (if the state information resources or critical information infrastructure parts support such functionality)	x	x	x	x	
14. The lists of people with the administrator-level access to the state information resources or critical information infrastructure shall be approved and periodically reviewed by a competent person or department responsible for the organization and management of cyber security. A list must be reviewed immediately when, in cases prescribed by law, the administrator is removed from work (duties)	x	x	x	x	
15. Administrator Account Control shall be performed:					
15.1. Periodically checking for unapproved administrator accounts				x	x
15.2. Administrator account controls are used to check administrator accounts. Unapproved accounts must be reported to the competent person or department responsible for the organization and management of cyber security	x	x	x		
16. State information resource or critical information infrastructure user account controls:					
16.1. Checking for unapproved user accounts to access state information resources or critical information infrastructure, and notifying a competent person or department responsible for the organization and management of cyber security about unapproved state information resources or critical information infrastructure user accounts	x	x	x	x	x
16.2. State information resources or critical information infrastructure user account controls are used to periodically check state information resources or critical information infrastructure user accounts. Unapproved accounts must be reported to the competent person or department responsible for the organization and management of cyber security	x	x	x		
17. It is forbidden to use the default passwords set by the manufacturer in the hardware and software used for state information resources or critical information infrastructure – they should be changed to conform with the requirements	x	x	x	x	x

Table 2. Audit and control of the state information resources or critical information infrastructure users and administrators

Requirement	CII	I	II	III	IV
18. This information shall be recorded for auditing purposes:					
18.1. Start-up / shutdown or restart of elements of the state information resources or critical information infrastructure (if such functionality is supported by parts of state information resources or critical information infrastructure)	x	x	x	x	x
18.2. Logins (and unsuccessful attempts to log in) / logouts of state information resources or critical information infrastructure users and administrators	x	x	x	x	x
18.3. Changes to state information resources or critical information infrastructure users / administrators the access rights to use system / network resources (if such functionality is supported by parts of the state information resources or critical information infrastructure)	x	x	x		
18.4. Activation / deactivation of the auditing function	x	x	x	x	x
18.5. Deletion, creation, or modification of audit logs	x	x	x	x	x
18.6. Modifiation of time and / or date	x	x	x		
19. The timestamps of audit logs shall be synchronized within the accuracy of at least one second	x	x	x		
20. At least two sources for time synchronization must be used	x	x			
21. Each audit log shall record:					
21.1. Date and exact time of the event	x	x	x	x	x
21.2. Event type / nature	x	x	x		
21.3. State information resources or critical information infrastructure user / administrator account information and / or state information resources or critical information infrastructure device, linked to a logged event	x	x	x	x	x
21.4. Event outcome	x	x	x	x	x
22. Tools that are used for the interface between state information resources or critical information infrastructure and a public digital communications network shall be designed to log all events related to incoming and outgoing data flows.	x	x	x		
23. Logged events in the state information resources or critical information infrastructure must be stored in hardware or software designed to store audit logs	x	x	x		
24. Due to various disruptions that impairs the capaibility to log events, the administrator and the competent person or department responsible for the organization and management of cyber security shall be informed immediately, but no later than one working day.	x	x	x		
25. Audit logs must be stored for at least sixty days, ensuring all significant content (for example, the user‘s identification data, whose employment relationship is terminated and who is removed from the	x	x	x		

system, identification data must be safely stored throughout the defined storage period for audit logs)					
26. It is forbidden to delete or change audit logs before the storage period for audit longs expires	x	x	x	x	x
27. Copies of audit logs must be protected against damage, accidental loss, unauthorized modification or destruction	x	x	x		
28. The use of audit logs must be controlled and recorded. Audit logs should only be available to the administrator and a competent person or department responsible for the organization and management of cyber security (including review rights)	x	x	x		
29. Audit logs shall be analyzed by the administrator at least once a month, and their results shall be delivered to a competent person or department responsible for the organization and management of cyber security	x	x	x		

Table 3. Intrusion Detection and Prevention

Requirement	**CII**	**I**	**II**	**III**	**IV**
30. Intrusion detection systems must be in place and operational to monitor incoming and outgoing data traffic and internal traffic between the most important network services of state information resources or critical information infrastructure	x	x	x	x	x
31. In case of a detected suspicious activity, the log event must be recorded in audit logs and a notifcation must be delivered to the administrator	x	x	x		
32. The generated message shall be classified according to the recorded event	x	x	x		
33. The attack signature must be updated using reliable sources of relevant information. Updated database of attacks signatures must be downloaded no later than twenty-four hours after the manufacturer releases the updated database of attack signatures, or no later than seventy-two hours after the manufacturer releases the updated database of attack signatures, if by the decision of a manager of state information resources or critical information infrastructure, a database of attack signatures is being installed and its impact assessement (testing) to state information resources and critical information infrastructure is being carried out	x	x	x		
34. Main servers must have enabled firewalls configured to block all incoming and outgoing traffic, except for traffic related to state information resources or critical information infrastructure functionality and management	x	x	x	x	x
35. Intrusion detection configuration and cyber incident detection rules must be stored digitalally separately from state information resources or critical information infrastructure hardware (including relevant dates (implementation, update an detc.), people responsible, application periods, and etc.)	x	x	x	x	x

Table 4. Wireless network security and control measures

Requirement	CII	I	II	III	IV
36. Only configured wireless network devices, which meet technical cyber security requirements, are allowed to be used only by a competent person or department responsible for the organization and management of cyber security	x	x	x	x	x
37. The following controls of wireless devices must be carried out:					
37.1. Wireless devices operating within the state information resources or critical information infrastructure must be controlled, and a competent person or department responsible for the organization and management cyber security shall be notified of any use of unauthorized or non-compliant wireless devices	x	x	x	x	x
37.2. Tools that are used to restrict the use of unauthorized or technically non-compliant wireless devices, must inform a competent person or department responsible for the organization and management of cyber security	x	x	x		
37.3. Only configured wireless access points approved by a competent person or department responsible for the organization and management cyber security are permitted to use	x	x	x	x	x
38. Wireless access points can only be installed in a separate sub-network or other controlled area	x	x	x	x	x
39. When connecting to a wireless network, the EAP (Extensible Authentication Protocol) / TLS (Transport Layer Security) protocol must be enabled.	x	x	x	x	x
40. The use of the SNMP (Simple Network Management Protocol) must be restricted in the wireless network interface	x	x	x	x	x
41. All unnecessary management protocols must be restricted	x	x	x	x	x
42. Unused TCP (Transmission Control Protocol) / UDP (User Datagram Protocol) ports must be disabled	x	x	x	x	x
43. Peer to peer functionality must be disabled to prevent wireless devices from communicating with each other	x	x	x	x	x
44. The wireless connection must be encrypted with at least 128-bit key	x	x	x	x	x
45. Before the wireless encryption starts, manufacturer‘s default key of a wireless Access point must be changed	x	x	x	x	
46. Wireless Access, peer to peer functionality and wireless peripheral access must be disabled on computers and mobile devices, if it is not necessary to carry out the regular functions,	x	x	x		

Table 5. Security and control measures for mobile devices used to connect to the state information resources or critical information infrastructure

Requirement	CII	I	II	III	IV
47. The security and control requirements for identification, authentication and the use of the state information resources or critical information infrastructure, as set out in Table 1 of this Annex, shall be applied in accordance with the categories of importance of the state information resources or critical information infrastructure.	x	x	x	x	x
48. Only mobile devices complying with security requirements set out by the manager of state information resources or critical information infrastructure may be used	x	x	x	x	x
49. The manager of state information resources or critical information nfrastructure must have the right to manage mobile devices and the software installed in them	x	x	x	x	
50. The following controls of mobile devices must be carried out:					
50.1. Mobile devices used with state information resources or critical information infrastructure shall be controlled, and a competent person or department responsible for the organization and management of cyber security shall be notified abour any use of unauthorized or non-compliant mobile devices	x	x	x	x	x
50.2. Tools used to restrict the use of unauthorized or non-compliant mobile devices must notify a competent person or department responsible for the organization and management of cyber security about the use of unauthorized or non-complaing mobile devicess to connect to the state information resources or critical information infrastructure.	x	x	x		
51. Mobile devices must have installed centrally managed and updated anti-malware software, and other detection, halting and monitoring tools.	x	x			
52. Operating system updates and other software updates recommened by the software vendor must be installed	x	x	x	x	x
53. Mobile devices must have executable code controls that restrict the use of unauthorized executable code or inform the administrator about the use of unauthorized executable code	x	x			
54. Securely configured mobile device OS image must be prepared. The image must contain only the necessary operating system components (administrator accounts, services, applications, network ports, updates, systematic measures). Images must be reviewed and updated regularly, and updated immediately if new vulnerabilities or attacks are detected	x	x	x		
55. Mobile devices must have installed a securely configured operated system that is based on a OS image	x	x	x		
56. Mobile devices used for browsing the Internet must be protected against mobile code threats	x	x	x		
57. Unathorized devices may not be connected to mobile devices	x	x	x		
58. By the decision of a manager of state information resources or critical information infrastructure, other devices may be connected to mobile devices. A list of devices permissibale to connect, prepared by an administrator together with a competent person or department responsible for the organization and management of cyber security, shall be approved by the manager of state information resources or critical information infrastructure	x	x			

59. Data transmitted between a mobile device and state information resources or critical information infrastructure must be encrypted using a virtual private network (VPN)	x	x	x	x	
60. Identity must be authenticated when accessing the state information resources or critical information infrastructure; it must be prohibited to save the password in the mobile device or in its used applications	x	x	x	x	
61. A portable device, receiving energy from an integrated energy source and capable of transmitting and / or receiving digital data transmitted through a physical medium, electromagnetic waves and light, must be automatically locked, if not used for a specified period of time (e.g. five minutes)	x	x	x		
62. Mobile devices must have an installed tool enabling to remotely and irreversibly erase data	x	x			
63. Data storage security must be ensured	x	x	x	x	x
64. Data must be encrypted on both: mobile device storage and external data storage	x	x	x		

Table 6. The security and control measures for a publically accesible (from digital communications networks) website of state information resources and critical information infrastructure

Requirement	**CII**	**I**	**II**	**III**	**IV**
65. Security and control requirements for identification, authentication and the use of state information resources or critical information infrastructure, as set out in Table 1 of this Annex, are implemented in accordance to categories of importance of state information resources or critical information infrastructure	x	x	x	x	x
66. Additional identification, authentication and access control requirements:					
66.1. It is forbidden to store passwords in a software code	x	x	x	x	x
66.2. Websites authenticating a remote user access must not store passwords	x	x	x	x	
67. Following web cryptography requirements must be applied:					
67.1. When administrating the website, the connection must be encrypted using at least a 128-bit key	x	x	x	x	x
67.2. Digital certificates used in encryption must be issued by trusted certification services. The certificate key must be at least 2048 bit long					
67.3. TLS (Transport Layer Security) standard must be used	x	x	x		
67.4. Web cryptographic features must be installed on a part of the server where the website is located, or on a hardware security module	x	x	x	x	
67.5. All cryptographic modules must be able to fail securely	x	x	x		
67.6. Cryptographic keys and algorithms must be managed in accordance with the requirements set by the communications and information system manager	x	x	x	x	x
68. Secure configuration of a server, where the wesbite is hosted, must be evaluated using the test tool recommended by the National Cyber Security Center	x	x	x		

69. It is prohibited to store session data (identifier) at the server after the end of the session	x	x	x	x	x
70. Web application firewall must be used. Attack signature database should be updated using reliable sources. Updated database of attacks signatures must be downloaded no later than twenty-four hours after the manufactured releases the updated database of attack signatures, or no later than seventy-two hours after the manufactured releases the updated database of attack signatures, if by the decision of a manager of state information resources or critical information infrastructure, a database of attack signatures is being installed and its impact assessment (testing) to state information resources and critical information infrastructure is being carried out	x	x	x		
71. Security measrues against major network attacks must be carried out incdluing: SQL injection, Cross-site scripting, denial of service (DOS), distributed denial of service (DDOS) and other attacks; the list of major network attacks can be found on the the Open Web Application Security Project (OWASP), on a website www.owasp.org	x	x	x		
72. Validation control of data entered by the user must be used	x	x	x	x	
73. The server, where the wesbite is located should not display error messages to the website user about the website's script or server	x	x	x	x	
74. Website security tools must be able to restrict access to the server from IP addresses, which are known for engaging in malicious activity (unauthorized attempts to connect, inserting SQL injections, and etc.)	x	x	x		
75. Audit log and control requirements set out in in Table 2 of this Annex are implemented according to the categories of importance of state information resources or critical information infrastructure	x	x	x	x	x
76. The server, where the website is hosted must allow HTTP methods to ensure the functionality of the website	x	x	x	x	x
77. Directory browsing must be restricted	x	x	x	x	x
78. Defacement monitoring tools must be installed	x	x	x		

Table 7. Internet security and control measures used by the state information resources or critical information infrastructure

Requirement	CII	I	II	III	IV
79 The manager of state information resources or critical information infrastructure shall have the following contracts with an Internet Service Provider(s):					
79.1. Response to cyber incidents during normal business hours	x	x	x	x	x
79.2. Response to cyber incidents after normal business hours	x	x	x		
79.3. Continuous internet service provision:					
79.3.1. during normal business hours				x	x
79.3.2. twenty-four hours a day, seven days a week	x	x	x		
79.4. Internet service outage recording:					
79.4.1. during normal business hours				x	x
79.4.2. twenty-four hours a day, seven days a week	x	x	x		
79.5. Denial of service (DoS) protection against state information resources or critical information infrastructure	x	x	x	x	x

_____

Added appendix:
No. 1209, 2018-12-05, published TAR 2018-12-10, i. k. 2018-20153