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

NATIONAL CYBER INCIDENT MANAGEMENT PLAN

CHAPTER I
GENERAL PROVISIONS

1. The National Cyber Incident Management Plan (hereinafter referred to as "the Plan") sets out procedures for cyber incident management while defining cyber incident categories, cyber incident information, cyber incident investigation and cyber incident analysis after cyber incident investigation is over.

2. The terms used in the plan are defined in the Law on Electronic Communications of the Republic of Lithuania, Law on Electronic Communications of the Republic of Lithuania, the Law on Cyber Security of the Republic of Lithuania, the Law on State and Service Secrets of the Republic of Lithuania and the Law on the Management of State Information Resources of the Republic of Lithuania.

3. The National Cyber Security Center under the Ministry of National Defense is responsible for the organization, monitoring and analysis of cyber incident management at a national level. The State Data Protection Inspectorate, the Lithuanian Police and other institutions whose functions are related to cyber security within the competence assigned by the the Law on Cyber Security investigates or participates in cyber incidents management.

4. The National Cyber Security Center, the State Data Protection Inspectorate, and the Lithuanian Police (hereinafter jointly referred to as the "cyber incident management and / or investigation authorities - the CIMI authorities, and separately - the CIMI institution) shall appoint persons to be contacted on a 24-hour basis and who shall be responsible for the exchange of information during cyber incident management, foresees their substitutability. The State Data Protection Inspectorate and the Lithuanian Police shall provide the National Cyber Security Center with telephone numbers, e-mail addresses, and other contact information of the responsible persons who can be contacted on a 24-hour basis, enabling the exchange of information during the cyber incident management.

5. The Office of the Government of the Republic of Lithuania, the Office of the Seimas of the Republic of Lithuania, the Office of the President of the Republic of Lithuania, the State Security Department of the Republic of Lithuania, the Ministry of National Defense of the Republic of Lithuania designate the persons responsible for the transmission of information according to the procedure established in the Plan and provide the contact information of these persons to the National Cyber Security Center.

6. Cyber security entities shall provide the National Cyber Security Center with with telephone numbers, e-mail addresses, and other contact information of the responsible persons who can be contacted on a 24-hour basis, enabling the exchange of information during the cyber incident management.

7. Due to a change of responsible persons or their contact information, the updated information shall be submitted no later than the next working day after the change of data according to the procedure set out in point 4 to 6 of the Plan.

CHAPTER II

CATEGORIES OF CYBER INCIDENTS

8. The categories of cyber incidents shall be determined by the impact on the communication and information systems and / or services of cyber security entities and / or the impact on the recipients of the services provided by the communication and information systems.

9. Cyber incidents are divided into four categories:

9.1. dangerous cyber incidents;

9.2. high impact cyber incidents;

9.3. medium-impact cyber incidents;

9.4. minor impact cyber incidents.

10. The criteria for assigning cyber incidents to the categories set out in point 9 of the Plan are set out in the Annex to the Plan.

11. Cyber incidents for the categories defined in subpoints from 9.2 to 9.4 of the Plan, taking into account the criteria set out in the Annex to the Plan, are attibuted by cyber security entities, in whose communication and information systems cyber incidents have occurred If a cyber incident and / or its impact meets at least one of the criteria of the dangerous cyber incident, that are listed in the Annex to the Plan, cyber security entities shall attribute cyber security incident as high impact cyber security incident, which is defined in point 9.2 of the Plan..

12. National Cyber Security Center is the only one which is entitled to attribute cyber incidents as a dangerous cyber incident as it is defined in subpint 9.1 of the Plan, if the the identified cyber incident and / or its impact meets at least one of the criteria of a dangerous incident, listed in the Annex to the Plan.

CHAPTER III
INFORMATION ABOUT CYBER INCIDENTS

13. Cyber security entities shall inform the National Cyber Security Center of:

13.1. high impact cyber incidents - immediately, but no later than one hour after their detection;

13.2. moderate impact cyber incidents - no later than four hours after their detection;

13.3. minor cyber incidents – periodically providing information on the number of incidents that occurred in each group since the date of the last report, on the first working day of each calendar month.

14. The National Cyber Security Center shall be informed about the major or moderate impact cyber incidents by a report of a cyber security entity, indicating:

14.1. the cyber incident group (s), subgroup (subgroups) and exposure category determined in accordance with the criteria indicated in the Annex to the Plan;

14.2. a brief description of the cyber incident;

14.3. the exact time at which the cyber incident occurred and was identified;

14.4. the cyber incident elimination procedure (indicating whether it is a priority or not);

14.5. the exact time when the cyber incident investigation report will be provided.

15. digitalsService providers shall only notify the National Cyber Security Center of high-impact cyber incidents and only when the digital service provider has access to the information necessary to assess the impact of the incident.

16. Critical information infrastructure managers whose provision depends on the services provided by the digital service providers, having a disruptive impact on the critical information infrastructure operations that they manage, caused by disruptions in the digital service providers' communications and information systems, immediately, but no later than within one hour after indication of the disruptive effect, inform the National Cyber Security

Center and the digital service providers in whose communications and information systems disruptions occured, about the disruptive effect.

17. Persons who are not obliged by law to report about cyber incidents that occurred in their communication and information systems have the right to voluntarily report to the National Cyber Security Center about cyber incidents and applied cyber incident investigation or management measures to the contacts indicated on the National Cyber Security Center website.

18. When information about the a cyber incident is received by a National cyber security center from persons who are not obliged to report about the cyber incidents that occurred in their communication and information systems, such cyber incident is categorized by a National cyber security center independently and is investigated in the same manner as cyber incidents that were reported by cyber security entities.

19. Taking into account the extent of cyber incident prevalence, the established criteria for assigning a cyber incident to the categories defined in points 9.2-9.4 of the Plan, or the impact of a cyber incident on the communications and information system, the National Cyber Security Center shall, upon receipt of information about a cyber incident, have the right to:

19.1. to clarify the category of cyber incident (by assigning a cyber incident to a higher or lower category);

19.2. to ask for a additional information, which shall be necessary to evaluate the cyber security status of the cyber security entity's communications and information system, by indicating the deadline by which information may be submitted.

20. National Cyber Security Center after assessing the information confirms, updates or assignes the category of the cyber incident independently as it is indicated in the point 9 of the Plan, and, no later than one hour after receiving information or, if the cyber security entity is asked for adittional information, after receiving additional information, informs the notifier.

21. When it is necessary to inform the society for the purposes to avoid cyber incidento or to manage cyber incident that is happening, National Cyber Security Center after the consultation with the cyber security entity, which reported about the cyber security incident, informs society about the particular cyber incident or insist on informing by the cyber security entity itself.

CHAPTER IV
INVESTIGATION OF CYBER INCIDENTS

FIRST SECTION
INVESTIGATION OF HIGH, MEDIUM AND INDEPENDENT CIBERNET INCIDENTS

22. Cyber security entities shall conduct cyber incident investigations in accordance with their approved cyber security legal acts, to the extent not covered by the Plan, and shall take all possible measures necessary for the management of the cyber incident and the normal operation of communication and information systems.

23. Cyber security entities shall submit to the National Cyber Security Center a cyber incident investigation report on:

23.1. high impact cyber incident management status - no later than four hours after their detection and at least every four hours updated information before the cyber incident is contained or terminated;

23.2. medium-impact cyber incidents management status - no later than twenty-four hours after its detection and at least twenty-four hours of updated information before the cyber incident is contained or terminated;

23.3. containment or termination of high or medium-impact cyber incidents - no later than four hours after their containment or termination.

24. Supplying high or medium-impact cyber incidents investigation report to the National cyber security center, report shall include information known to the cyber security entity:

24.1. the cyber incident group (s), subgroup (subgroups) and exposure category determined in accordance with the criteria indicated in the Annex to the Plan;

24.2. type of communication and information system in which the cyber incident is detected (electronic communications network, information system, register, industrial process management system, server station and the like);

24.3. the duration of the cyber incident;

24.4. source of cyber incident;

24.5. features of a cyber incident;

24.6. method of cyber incident operation;

24.7. the possible and / or established consequences of a cyber incident;

24.8. the extent of the occurrence (potential spread) of cyber incident effects;

24.9. cyber incident status (active, passive);

24.10. the measures which were used to identify cyber incident;

24.11. possible and / or applicable cyber incident management measures;

24.12. the exact time at which the cyber incident report will be repeated on the basis of point 23 of the Plan.

25. Cyber security entities who have assessed that they will not be able to independently investigate or contain a cyber incident within the maximum permissible time of service failure specified in their approved cyber security legislation shall seek the assistance of the National Cyber Security Center no later than twenty-four hours after such circumstances have been established.

26. The National Cyber Security Center shall take the necessary steps to investigate the cyber incident and to identify all the circumstances described in the cyber security report:

26.1. high impact cyber incident investigations are launched immediately on the same business day when a notification from a cyber security entities is received;

26.2. Medium-impact cyber incidents investigations shall be initiated only after a high impact cyber incident investigation is completed, but no later than three working days after the notification about the cyber security incident is received from the cyber security entities.

27. The monitoring of minor impact cyber incidents shall be performed by the National Cyber Security Center and by cyber security entities. If minor impact cyber incidents are attributed to the category of cyber incidents of higher significance in the manner prescribed in the Plan, they shall be investigated in accordance with the requirements set out in the Plan.

28. The investigation of high or medium-impact cyber incidents is completed and the cyber incident is considered to be cointained or terminated when the impact of the cyber incident on the communication and information system is eliminated and / or the normal operation of communication and information systems, which meets the criteria, established in cyber security legislation of the cyber security entities, is restored .

29. Cyber security entities shall, at the latest within eight hours after the cyber incident has been contained or terminated, inform the recipients of the services provided by the communication and information system, if there are any, if the impact of the cyber incident has caused or is likely to cause harm to the recipient of the communications and information system services.

SECOND SECTION
INVESTIGATION OF DANGEROUS CYBER INCIDENTS

30. The National Cyber Security Center, having assigned a cyber incident to the category of a dangerous cyber incident, taking into account cyber security situation, shall immediately, but no later than one hour after the received information on a dangerous cyber incident, inform the other CIMI institutions on the basis set out in subpoints 44.2-44.3 of the Plan and shall indicate the cyber security entities that the cyber incident must continue to be investigated and managed in accordance with legislation approved by the cyber security entity, or takes over the investigation and / or management of a dangerous cyber incident.

31. Cyber security entities, following the instructions of the National Cyber Security Center and continuing to investigate and manage a dangerous cyber incident, at least every four hours provide the National Cyber Security Center with updated information on the status of the management of a dangerous cyber incident, consisting of the information specified in point 24 of the Plan. The National Cyber Security Center, taking into account the information provided by cyber security entities, has the right to take over the investigation and / or management of a dangerous cyber incident.

32. After the National Cyber Security Center has taken over the investigation and / or organizing the management of a dangerous cyber incident, cyber security entities shall:

32.1. continuously collect, processes information related to a cyber incident and provide it to the National Cyber Security Center at least every four hours;

32.2. provide the National Cyber Security Center with the information about the the work carried out on investigating and / or managing cyber incidents and their results at least every four hours. Information shall consist of the information specified in point 24 of the Plan;

32.3. implement the instructions, concerning the organization of cyber incident investigation and / or management, of the National Cyber Security Center, and participates in the cyber incident management process through implementing cyber security measures.

33. The National Cyber Security Center, having taken over the cyber incident investigation and / or management organization, shall take the necessary steps to investigate the cyber incident and examine all circumstances referred by the cyber security entities:

33.1. assesses cyber incident information provided by cyber security entities;

33.2. makes decisions on investigation and / or management of a cyber incident;

33.3. provides cyber security entities with instructions related to cyber incident investigation and / or management;

33.4. has the right to organize a coordination meeting on cyber incident investigation and / or management, which must involve representatives of the relevant CIMI institutions, competent persons appointed by the cyber security entities, responsible for cyber security organization and ensurance, and other representatives of cyber security entities,who are required to participate in order to contain cyber incident. The National Cyber Security Center has the right to invite other competent experts to the coordination meeting.

34. If several cyber security incidents occur at the same time, the National Cyber Security Center primarily investigates and manages those dangerous cyber incidents that cause or may cause the most damage.

35. The National Cyber Security Center, having investigated that the organizer (s), executor (s) or source of a dangerous cyber incident is outside the territory of the Republic of Lithuania, has the right to apply for assistance and provide information related to the cyber incident to other institutions of other states or international organizations that perform cyber security functions and collaboration with whom is taking place.

36. The National Cyber Security Center shall inform the responsible persons appointed by the Government, the Seimas and the Office of the President chancellery and the Ministry of National Defense immediately, but no later than within one hour after the cyber incident has been classified as a dangerous cyber incident, about the investigation and / or management action and, within four hours of the cyber incident categorization as a dangerous cyber incident, provide a report on a summary of the dangerous cyber incidents ,containing the information specified in point 24 of the Plan.

37. The chancellery of the Government, the Parliament and the President, having assessed the information on a dangerous cyber incident, shall inform the heads of theinstitutions, the Prime Minister, the Speaker of the Parliament and the President, respectively.

38. The National Cyber Security Center shall inform the recipients of the information referred to in point 36 of the Plan regularly, at least every four hours, of the investigation and / or management of a dangerous cyber incident by providing an updated report on the investigation of dangerous cyber incidents and information on the containment or termination of a dangerous cyber incident shall be provided to these recipients and the cyber security entity at the latest within one hour of the containment or termination of a dangerous cyber incident. The investigation of a dangerous cyber incident is completed and a cyber incident is considered to be containes or terminated when the impact of the cyber incident on the communications and information system is eliminated and / or the normal operations of the communication and information system that meet the criteria established by cyber security entites in their cyber security legislation are restored.

39. The National Cyber Security Center, having determined that CIMI institutions and cyber security entities have not enough available resources in order to investigate and / or contain dangerous cyber incident, immediately, but not later than within one hour after the determination of these circumstances, informs the responsible persons appointed by the chancellery of the Government and the Ministry of National Defense as well as the Minister of National Defense, who, accordingly, decides on the investigation and / or measures of a dangerous cyber incident no later than twenty-four hours

40. If the containment of dangerous cyber incident by applying the additional measures appointed by the Minister of National Defence has failed, the National Cyber Security Center shall inform the Minister of National Defense and the responsible person appointed by the chancellery of the Government without delay, but not later than within one hour after such circumstance is determined, by submitting a report on the investigation of dangerous cyber incidents.

41. The Minister of National Defense shall submit a draft resolution to the Government of the Republic of Lithuania, proposing that the cyber incident be recognized as a cyber security crisis, no later than twenty-four hours after receipt of the information specified in point 40 of the Plan.

SECTION THREE
INTERINSTITUTIONAL COOPERATION AND EXCHANGE OF INFORMATION ON INVESTIGATION OF CYBER INCIDENTS

42. The CIMI institutions, having identified a possible cyber incident in the cyber security entity's communications and information systems, shall inform the cyber security entity without delay, but not later than four hours after such circumstances have been identified.

43. Cyber security entities, after receiving information from the CIMI institutions, other legal entities or other states or international organizations or other institutions that perform cyber security functions about the possible cyber incident detected in their communications and information systems shall take action to detect and confirm a cyber incident. In the absence of cyber incident features, cyber security entities will inform the CIMI institutions no later than four hours after receiving a cyber incident notification.

44. Upon a receipt of information on a cyber incident, the CIMI authority shall inform the other CIMI institutions immediately, but no later than twenty-four hours after receipt of information on the cyber incident:

44.1. National Cyber Security Center - having identified that cyber incident may also affect cyber security entities’ communications and information systems;

44.2. The Lithuanian Police - having identified that a cyber incident may have ifeatures of cyber crime;

44.3. The State Data Protection Inspectorate - having identified that a cyber incident may be related toa personal data breach.

45. The CIMI authority investigating a cyber incident within its competence, having identified the need for additional information on a cyber incident, shall have the right to apply to other CIMI institution or cyber entities who have obligation to submit additional information within the time limit specified in the request of the CIMI authority, which is competent for cyber incident investigation.

46. Cyber security entities and CIMI institutions shall transmit the information related to cyber incidents and their management and specified in this Plan via the cyber security information network and, if there is no such possibility , by other secure means of communication.

47. At the request of the State Security Department, the National Cyber Security Center shall, no later than seven working days after receipt of such a request, inform the responsible person designated by the State Security Department of high impact and dangerous cyber incidents through the cyber security information network, or, if there is no such possibility, by other secure means of communication.

48. The CIMI institutions, having received information from other states or international organizations or institutions that perform cyber security functions, about cyber incidents occurring in other states that could be classified as high-impact or dangerous, shall immediately, but no later than within one hour after being aware of these circumstances provides information on the cyber incident to cyber security entities that may be affected by a cyber incident occurring in other states.

SECTION FOUR
INTERNATIONAL COOPERATION AND EXCHANGE OF INFORMATION IN INVESTIGATION OF CYBER INCIDENTS

49. The National Cyber Security Center shall coordinate the exchange of data and information that it is transmitted between other states or international organizations or institutions that perform cyber security functions, the CIMI institutions and cyber security entities.

50. The National Cyber Security Center, while coordinating international and interinstitutional cooperation activities:

50.1. ensures cross-border cooperation between the institutions of the Republic of Lithuania and other Member States of the European Union and cooperation with the the Cooperation Groups of these states, Computer security incident response teams (CSIRTs) and other institutions in order to perform effective cyber security supervision and exchange information among the stakeholders expeditiously;

50.2. informs the European Commission about the extent of the cyber incident management process (indicating post-cyber incidents groups, impact, number, cyber incidents that potentially affected bother European Union countries, and other relevant information) and key elements, and submits summary reports annually to the Cooperation Group on notifications received, which includes, inter alia, the number of notifications and the nature of the incidents reported, as well as the actions taken;

50.3. informs other Member States of the European Union, their CSIRTs about dangerous and high-impact cyber incidents when the provision of critical information infrastructure services may be affected in more than one Member State;

50.4. provides cyber security early warnings, warnings and recommendations to stakeholders.

51. When coordinating international and interinstitutional cooperation activities, the National Cyber Security Center shall have the right to exchange information provided by cyber security entities, including confidential information and commercial secrets, to the extent necessary for the coordination of international and interinstitutional cooperation and ensures the protection of the information received.

52. With the approval of the Minister of National Defense, the National Cyber Security Center, when performing the functions set out in the Plan, shall have the right to involve competent authorities of international organizations, Cooperation Groups established by them and Competent Authorities and Services of foreign states. The National Cyber Security Center is responsible for the activities of the competent authorities of the international organizations involved, the Cooperation Groups established by them and the CompetentAuthorities and Services of foreign states in the performance of their functions in the Republic of Lithuania.

CHAPTER V
ANALYSIS OF CYBER INCIDENTS AFTER THE CYBER INCIDENT INVESTIGATION IS OVER

53. Cyber security entities and CIMI institutions shall carry out an analysis after the containment or termination of cyber incident. For cyber incidents attributed to a category of minor impact, no cyber incident analysis is performed.

54. A cyber security entity in whose communication and information system cyber incident has been investigated , having analyzed and evaluated all information related to the cyber incident, and the actions that were carried out and measures taken:

54.1. not later than thirty working days after the cyber incident has been contained or terminated, submit the results of the cyber incident analysis to the National Cyber Security Center and publish a structured and up-to-date non-classified information on cyber incident detection and containmentin the Cyber security information network;

54.2. take steps to remove vulnerabilities in the communications and information system;

54.3. assesses the risk of communication and information system and compliance with Organizational and technical cyber security requirements established by the Government;

54.4. by identifying legal gaps, replaces its cyber security legislation and / or initiates amendments to legislation adopted by other institutions.

55. The CIMI institutions shall have the right to require cyber security entities to provide additional information required for the analysis of the cyber incident no later than thirty working days after the cyber incident has been contained or terminated.

56. The CIMI institutions after analyzing and evaluating all information related to the cyber incident, actions carried out and measures taken:

56.1. replace legislation (initiates legislative changes), regulating cyber security by identifying insufficient legal regulation;

56.2. initiate, as appropriate, amendments to the Critical Information Security Plan for Critical Information Infrastructures;

56.3. assess the need for improvement or updating of organizational and technical cyber security measures, plan measures to meet this need and ensure their implementation.

57. The National Cyber Security Center, after conducting a cyber incident analysis or receiving the results of a cyber incident analysis from cyber security entity or CIMI institution, shall publish a structured non-classified cyber-incident information on the cyber incident analysis no later than thirty working days after receipt of this information in the cyber security information network or on its website.

_____

LIST OF CRITERIA, USED FOR CALSSIFICATION OF CYBER INCIDENTS TO CYBER INCIDENTS CATEGORIES

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)		
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
1.	Diseminatio n of abusive content, spam.	1.1. Spam and (or) disemination of abusive content disturbe CIS activity and (or) provided services	N				V					D					P		
		1.2. Disemination of abusive content, spam	N																
2.	Malicious software / code) Software or its part, which helps to connect to CIS	2.1. Advanced persistent threat (APT) is detected					V					D					P		
		2.2. CIS is actively controlled by intruders (for example, back door), computerized working places or servers become part of Botnet infrastructure					V					D					P		

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria): CIS disturbance < 1 hour.	Minor (N): Number of affected users or computerized work place < 100, or 5 %	Minor (N): Service is provided, but disturbed	Minor (N): Losses < 250 000 Eur	Medium-impact (V) (two or more criteria): CIS disturbed ≥ 1 hour, but < 2 hour	Medium-impact (V): Number of affected users or computerized work place < 1000, or 25 %	Medium-impact (V): Service is provided in a part of state teritory	Medium-impact (V): Breach of the information or CIS confidentiality and (or) integrity	Medium-impact (V): Losses ≥ 250 000, but < 500 000 Eur	High-impact (D) (two or more criteria): CIS disturbed ≥ 2 hour	High-impact (D): Number of affected users or computerized work place ≥ 1000, or 25 %	High-impact (D): Service is provided in a whole state teritory and (or) ≥ 1 EU state	High-impact (D): Breach of the information or CIS confidentiality and (or) integrity	High-impact (D): Losses ≥ 500 000 Eur	Dangerous (P) (at least one of the criteria): CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Dangerous (P): Number of affected users or computerized work place ≥ 100 000, or 50 %	Dangerous (P): Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	illegally, gain control, disturb or modify their functioning, to destroy, damage, delete or modify electronic information, to remove or restrict possibility to use electronic information	2.3. Malicious software / code, disturbing activity of security measures					V					D					P		
		2.4. Malicious software / code, which is detected by the security measures during the regular check and (or) is blocked automatically by the security measures	N				V												
		2.5. Malicious software / code, which is disseminated by using methods of social engineering	N				V					D					P		

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)		
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	and misappropriate or use non-public electronic information in another way by non-authorised persons																		
3.	Information gathering	3.1. Takeover of CIS packages / information					V					D					P		

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)		
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	Intelligence or other scanning, sniffing activity, manipulation of users emotions, psychology, poor level of attention, taking advantage in lack of technological awareness	3.2. CIS counterfeiting in order to gather access or other important information, targeted emails, which aims at cheating out access and (or) other important information by using social engineering methods, convincing to commit desirable actions (for example, financial operations)					V					D					P		
		3.3. Intelligence of perimeter measures has been carried out (not attempting to hack)	N				V												
		3.4. Social engineering methods have been carried out in order to gain access to CIS	N				V												

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)		
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	(social engineering) in order to track and gather information, to reveal gaps, to perform destructive activities, deception in order to perform phishing against user or convince	and (or) gain any other important information																	

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)		
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	him to commit desirable actions																		
4.	Intrusion attempts Intrusion attempts or attempt to disturb CIS activity by exploiting of known vulnerabilities, by login attempts, by	4.1. One or more unknown zero-day vulnerabilities are being exploited in order to disturb particular CIS					V					D					P		
		4.2. One or more unknown zero-day vulnerabilities are being exploited	N				V					D					P		
		4.3. Interior CIS intelligence or other malicious activity (port scanning, login attempts, dissemination of malicious software and other)					V					D					P		

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)		
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	using other new attack signature	4.4. Known and publicly distributed vulnerabilities are being exploited or attempts to access to CIS by login attempts are being performed	N				V												
5.	Intrusions Successful intrusion and (or) illegal CIS usage, privileged account compromise, unprivileged account	5.1. Actions against CIS or its security measures, misappropriation of information, destruction, breach of CIS or its part, which disturbs uninterrupted provision of CIS' services and may influence integrity of processed information and provided services, modify content and lessen trust of CIS users					V					D					P		

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)			
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	compromise, application compromise	5.2. Illegal access to CIS, software applications or service is gained					V					D					P			
6.	Disturbance of services, availability breaches Actions, which disturb CIS activity, provided services (DoS (DdoS) attacks), breach of	6.1. Termination of provided services or exeeded maximum permitted inaction of a service					V					D					P			
		6.2. Disturbance of uninterrupted provision of services, which may influence accessibility to the processed information and (or) provided services	N				V													
		6.3. Disturbance of service is detected, which doesn't influence services provision	N				V													

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)		
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	CIS or its part, wchich disturb CIS activity and (or) its provided services (sabotage, outage)																		
7.	Breaches of information content security Unauthorised access to information, unauthorise	7.1. Unauthorised access to information, which may influence CIS activity and (or) provided services					V					D					P		
		7.2. Unauthorised access to information, unauthorised modification of information	N				V					D					P		

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)		
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	d modification of information																		
8.	Illegal activity, fraud Theft, deception, unauthorized use of resources, illegal usage of software or copyright infringement, identity	8.1. Illegal influence to CIS and (or) provided services	N				V					D					P		

Serial No	Cyber incident groups	Impact of cyber incident / Cyber incident subgroups	Minor (N) (at least one of the criteria)				Medium-impact (V) (two or more criteria)					High-impact (D) (two or more criteria)					Dangerous (P) (at least one of the criteria)		
			CIS disturbance < 1 hour.	Number of affected users or computerized work place < 100, or 5 %	Service is provided, but disturbed	Losses < 250 000 Eur	CIS disturbed ≥ 1 hour, but < 2 hour	Number of affected users or computerized work place < 1000, or 25 %	Service is provided in a part of state teritory	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 250 000, but < 500 000 Eur	CIS disturbed ≥ 2 hour	Number of affected users or computerized work place ≥ 1000, or 25 %	Service is provided in a whole state teritory and (or) ≥ 1 EU state	Breach of the information or CIS confidentiality and (or) integrity	Losses ≥ 500 000 Eur	CIS disturbed ≥ 24 hours and (or) maximum permitted inaction of a service is exceeded	Number of affected users or computerized work place ≥ 100 000, or 50 %	Services are (may be) disturbed in a whole state territory and (or) ≥ 1 EU state, state functions and (or) delivery of state commitments, emergency situation, which is indicated in the List of of emergency situations, approved by the Government, has occured (or may occure)
	fraud, deception and other incidents of of a similar nature																		
9.	Other Incidents, which does not qualify for any of the descriptions of the referred groups		N				V					D					P		