The Government of the Republic of Croatia

1399

Pursuant to Article 30 paragraph 2 of the Act on the Government of the Republic of (»Official Gazette «, No. 150/11, 119/14 i 93/16) and Article 20 of the Act on cybersecurity of operators of essential services and digital service providers (»Official Gazette «, No. 64/18), the Government of the Republic of Croatia at its session on 26 July 2018 passed the

REGULATION ON CYBERSECURITY OF OPERATORS OF ESSENTIAL SERVICES AND DIGITAL SERVICE PROVIDERS

PART I GENERAL PROVISIONS

Subject of the Regulation

Article 1

This Regulation establishes the measures for achieving a high level of cybersecurity of operators of essential services, the implementation model, the criteria for identifying incidents with a significant impact on the provision of essential services, the content of notifications and other key issues for incidents notification.

Harmonization with the EU legislation

Article 2

(1) This Regulation transposes into the legislation of the Republic of Croatia the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19 July 2016).

(2) This Regulation ensures the implementation of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a significant impact (OJ L 26/48, 31 January 2018 – hereinafter referred to as: Commission Implementing Regulation).

Definitions

Article 3

Particular notions within the meaning of this Regulation shall have the following meaning:

1) »Act« – is the Act on cybersecurity of operators of essential services and digital service providers

2) »operator of essential services« – is the operator identified as operator of essential service by the Decision referred to in Article 9 of the Act

3) »digital service provider« – is any private entity providing a digital service from the List in Appendix II of the Act within the European Union and which either has their head office or their

representative on the territory of the Republic of Croatia, under the condition that such provider does not represent a micro or small sized enterprise as defined by the Act stipulating the basis for the implementation of economic incentives aimed towards development, restructuring and market adaptation of small sized enterprises
4) »incident« – is any event having an actual adverse effect on the security of network and information systems referred to in Article 17 of the Act
5) »business continuity in providing services« – is the capability of providing a service without disruption or restoring the service at acceptable predefined level following a disruptive incident
6) »service user« – any individual or legal entity to whom the service is provided based on the regulation or legal arrangement
7) »system user« – any individual with an open account on the essential system
8) »responsible person« – head, management board member, director or chief executive officer
9) »competent CSIRT« – is the CSIRT competent at sectoral level in accordance with the List of competent authorities from Appendix III of the Act
10) »competent sectoral authority« – is the competent sectoral authority in accordance with the List of competent authorities from Appendix III of the Act
11) »single national point of contact« – Office of the National Security Council.

PART II
MEASURES FOR ACHIEVING A HIGH LEVEL OF CYBERSECURITY OF OPERATORS OF ESSENTIAL SERVICES

CHAPTER I
MANAGING THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

Management framework
Article 4

Operators of essential services shall establish the system of managing the security of network and information systems referred to in Article 17 of the Act (hereinafter referred to as: essential systems).

Security principles
Article 5

Functionality and security of essential systems shall be based on the following principles:
–confidentiality: property ensuring that services or information shall not be made available or disclosed to unauthorized persons
– integrity: property ensuring that services or information shall not modified in an unauthorized or undetected manner
– availability: property ensuring that service or information shall be accessed or used only upon request of the authorized user

– authenticity: property ensuring that the user identity is indeed the one that is claimed to be.

Establishing and documenting management policies
Article 6

(1) Operators of essential services shall establish and document the security management policy of essential systems.
(2) Security management policy of essential systems shall:
– define the objectives and strategic guidelines in order to preserve business continuity
– be based on risk assessment and risk management
– describe the security management system, including internal oversight of the implementation of cybersecurity measures
– establish the adoption of the necessary security operating procedures for essential systems, with links to other internal regulations stipulating the existing security operating procedures, whether they refer to essential systems or the security of operators in general
– include the organization and implementation of education programs and continuous enhancement of security awareness.
(3) Security management policy of essential systems shall be adopted in writing and shall be authorized by the highest management level.

Organizational structure
Article 7

(1) Operators of essential services shall appoint the person with the highest managing authority who shall be responsible for establishing and managing the security of essential systems.
(2) Operators of essential services shall establish the organizational structure, with formal division of duties, authorities and responsibilities, which shall ensure the appropriate security management of essential systems.

Internal oversight implementation
Article 8

(1) Operators of essential services shall establish the system of internal oversight of the implementation of cybersecurity measures defined by the security management policy of essential systems, whereas the internal oversight tasks shall be organizationally separate from the organizational structure responsible for essential systems.
(2) The internal oversight referred to in paragraph 1 of this Article shall be implemented at least once a year.
(3) The results of internal oversight referred to in paragraph 1 of this Article shall be forwarded, in writing, to the responsible person referred to in Article 7, paragraph 1 of this Regulation.
(4) The responsible person referred to in Article 7, paragraph 1 of this Regulation shall ensure the implementation of cybersecurity measures in accordance with the results of internal oversight referred to in paragraph 1 of this Article.

CHAPTER II
RISK MANAGEMENT

Establishing risk management system
Article 9

(1) Operators of essential services shall establish the risk management system for the essential system affected.
(2) Risk management system referred to in paragraph 1 of this Article shall include:
– methodology of determining the risks caused by incidents
– defining the persons responsible for the implementation of regular assessment of risks caused by incidents
– drafting or selecting the catalog of applicable risks and its update
– accepted method of risk treatment (avoidance, mitigation, transfer or risk acceptance)
– list of residual risks
– the procedure for adopting a formal decision on accepting residual risks by the highest management level.

Risk assessment
Article 10

(1) Operators of essential services shall implement the measures for preventing and mitigating the impact of incidents in proportion to the assessment of risk posed to their essential system.
(2) Operators of essential services shall implement the activities related to development, update and maintenance of essential systems, taking into account the results of assessment of risks posed to their essential system.

Article 11

(1) Operators of essential services shall continuously update the risk catalogue, taking into consideration the external and internal threats, newly discovered vulnerabilities, loss of effectiveness of the existing measures for preventing and mitigating the impact of incidents, changes of risks due to changes in information systems' architecture, all changes affecting the security of essential systems, as well as the results of previous risk assessments.
(2) Operators of essential services shall, at least once a year, perform the assessment of risks posed to their essential system and adopt the decision on accepting residual risks.

Identifying the equipment, personnel and activities in relation to risk assessment performance
Article 12

(1) Operators of essential services shall identify:
– the equipment comprising the essential systems
– the persons having the right to access essential systems and
– business activities performed in the essential systems or which support essential systems.
(2) Operators of essential services shall, by means of risk assessment, include all the identified elements referred to in paragraph 1 of this Article.

Incident prevention, detection, handling and mitigating the impact of incidents
Article 13

(1) Risk assessment shall be performed for identified equipment, personnel and activities referred to in Article 12 of this Regulation.
(2) Risk assessment shall be performed on the basis of the accepted risk catalogue with the requirement of risk assessment at least for the areas of essential systems' protection defined in Chapter III of this Regulation.
(3) The assessed risks shall be processed by avoidance, mitigation, transfer or acceptance.
(4) The assessed security risks shall be processed by a selection of various security measures and controls from the appropriate international information security standard.
(5) Security measures and controls from the appropriate international information security shall enable the following: deterrence, avoidance, prevention, detection, reaction and recovery, acting in an appropriate manner to threats and vulnerabilities of essential systems, that is the impact of incidents on essential systems.

Risk assessment documentation
Article 14

Operators of essential services shall protect the documentation generated by the implementation of assessment of risks posed to their essential system in a way which enables access only to authorized personnel.

CHAPTER III
AREAS OF ESSENTIAL SYSTEMS' PROTECTION

Physical and environmental security
Article 15

Operators of essential services shall ensure the implementation of measures related to physical and environmental security of essential systems from damage caused by system failure, human error, malicious action or natural phenomena.

Security of supplies
Article 16

(1) Operators of essential services shall ensure the availability of equipment, materials, energy products and other resources necessary for the regular and uninterrupted functioning and maintenance of essential systems.
(2) The supply chain of resources referred to in paragraph 1 of this Article shall include the security assessment of all selected contractors and subcontractors, as well as tracking the sources of resources purchased.

Contractual relationships' management
Article 17

(1) Operators of essential services shall regularly assess and reduce to acceptable level the risks resulting from contractual relationships with individuals and legal entities, the execution of which may have an impact on essential systems.

(2) Operators of essential services shall continuously monitor the means and quality of providing contracted jobs and services, which may have an impact on essential systems.
(3) Operators of essential services shall implement the risk assessment process before executing the contractual relationship with individuals and legal entities, whose activities may have an impact on essential systems.

Outsourcing Management
Article 18

(1) Operators of essential services, who use an external service provider for management and/or maintenance of essential system, shall regularly assess and reduce to an acceptable level the risks that may occur within the service outsourcing.
(2) Operators of essential services shall be responsible that the service provider referred to in paragraph 1 of this Article fully implements the measures for the protection of essential systems stipulated by this Regulation.
(3) Operators of essential services shall asses the risk of outsourcing of services prior to concluding the service provision contract.
(4) Contracts referred to in paragraph 3 of this Article shall contain a clause on the obligation to enable unrestricted oversight by the competent sectoral authority.
(5) Contracts referred to in paragraph 3 of this Article shall contain a clause on the obligation to continue providing the service even after the contract is terminated during a reasonable period of time, which shall enable the operator of essential services to conclude a contract with another external service provider or to organize autonomous service provision.

Access control to premises
Article 19

(1) Operators of essential services shall ensure the implementation of measures that ensure authorized and restricted physical and logical access to premises where essential systems are located, based on operational and/or security requirements.
(2) Operators of essential services shall identify and continuously update access control procedures referred to in paragraph 1 of this Article, which shall include at least the following:
– defining the list of persons with access rights
– entry procedures for persons without permanent access rights
– oversight of access control.

Physical and logical separation of essential systems
Article 20

(1) Operators of essential services shall implement the physical and/or logical separation of essential systems from all other network and information infrastructures.
(2) When physical and/or logical separation of essential systems is not possible, the operators of essential services shall, in accordance with the risk assessment:
– implement the measures to mitigate residual risk that occurred due to impossibility of complete separation
– document and accept residual risks
– document all essential system points where separation is not possible.

Essential system access controls
Article 21

(1) Operators of essential services shall ensure the implementation of measures which ensure authorized and restricted physical and logical access to essential systems, based on operative and/or security requirements.
(2) Operators of essential services shall identify and continuously update access control procedures for essential systems, which shall include at least:
– access control procedures and systems which include the use of unique personal identifiers and ensure the authentication procedures
– mechanisms of access control to essential systems, which shall ensure access only by authorized users, in accordance with operative and/or security requirements
– management system of user access rights, which shall include identification, authentication, authorization, registration, as well as permanent control of user access rights
– system of permanent monitoring of access to essential systems, which shall at least include authorization and control of access rights, monitoring and reporting in case of unauthorized access attempts
– administrator access to essential systems implemented in accordance with the rules which guarantee the use of hardware, software and online environment intended solely for administrator access
– regular assessment of effectiveness of access control procedures and rules and their upgrade, if necessary
– regular revision of dedicated access rights and their withdrawal in case the need no longer exists.

Essential systems activity log
Article 22

(1) Operators of essential services shall use the system for monitoring and tracking user activities on the essential system.
(2) Types of recorded logs shall at least include system users' login and logout, user accounts' opening and closing, user rights changes, changes of system security rights and the information on system functioning covering the respective servers.
(3) Each recorded system log for monitoring and tracking user activities shall include at least:
– identity of system user
– type of log
– time of log
– logical location of the essential system that the log refers to.
(4) System for monitoring and tracking user activities shall:
– enable collection of information on user activities from all parts of essential system
– be separate from the system where information is collected and
– be organized in such a way as to minimize the possibility of unauthorized alteration of user activity logs.
(5) Operators of essential services shall ensure permanent monitoring of activities and performing log analysis in case of incidents.
(6) Logs in the system for monitoring and tracking user activities shall be kept at least for the last 6 months.

Protection of information processed, stored and transmitted in the essential system
Article 23

(1) Operators of essential services shall ensure the implementation of protection measures for information processed, stored and transferred in the essential system, with the objective of protecting confidentiality, availability and integrity of information.
(2) Operators of essential services shall identify sensitive information that need to be protected by cryptographic mechanisms during their processing, storage and transfer in the essential system, with the objective of protecting confidentiality, availability and integrity of information.
(3) Operators of essential services shall appropriately apply the measures referred to in paragraphs 1 and 2 to portable media used for processing, storage or transfer of information in the essential system.

Protection from malware
Article 24

(1) Operator shall protect the essential system from malware by means of implementing the appropriate security measures and controls.
(2) Security measures and controls referred to in paragraph 1 of this Article shall ensure the identification and disabling of malware in the essential system, as well as recording and storage of information necessary for identifying the functionality disruption of essential system and continuity maintenance of the essential service.

Protection from disruption of availability of essential system
Article 25

(1) Operator shall protect the essential system from computer attacks that may disrupt its availability by means of implementing the appropriate security measures and controls.
(2) Security measures and controls referred to in paragraph 1 of this Article shall ensure identification and disabling of computer attacks that may disrupt the essential system's availability as well as recording and storage of information necessary for identifying the functionality disruption of essential system and continuity maintenance of the essential service.

Development and maintenance of essential systems
Article 26

(1) Operators of essential services shall define the means, criteria and procedures for essential systems development, with special emphasis on the importance of considering security aspects from the initial project phase, in accordance with the adopted project management methodology.
(2) Operators of essential services shall, within the process of essential system development, establish and document the process of system development and delivery, which includes analysis and design, software development, testing and introduction into production planning.
(3) Operators of essential services shall separate in appropriate manner the development, testing and production environment.
(4) Operators of essential services shall ensure that all developed software components in the essential system, as well as new hardware components of the essential system, before being introduced into production, are appropriately tested and approved by the responsible persons.
(5) Operators of essential services shall ensure that, before introducing any software component of the essential system into production, vulnerability checks and penetration tests are performed.

Project management
Article 27
(1) Operators of essential services shall identify the criteria, methods and procedures of project management of development and maintenance of essential systems referred to in Article 26 of this Regulation.
(2) Operators of essential services shall, for each project referred to in paragraph 1 of this Article, appoint the responsible person and project team.

Hardware management
Article 28
(1) Operators of essential services shall manage the essential system's hardware during their entire life cycle.
(2) The process of hardware management shall include identification, recording, usage, maintenance, write-off and controlled destruction of property.

Software change management
Article 29
(1) Operators of essential services shall manage the software changes of essential systems.
(2) The process of software change management shall include at least:
– identification of the existing software versions of the essential systems
– identification and tracking all software version changes of the essential system that impact or may impact the functionality and/or security of the essential system
– recording all software version changes of the essential system in order of their appearance, along with the time of their appearance.
(3) Operators of essential services shall, for each significant software version change of the essential system, in accordance with risk assessment, perform vulnerability assessment and penetration test.

Essential systems configuration
Article 30
(1) Operators of essential services shall ensure that:
– essential systems contain only hardware and software necessary for unhindered functioning and security of the system and
– only necessary data traffic is permitted on the essential system.
(2) In case the condition referred to in paragraph 1 of this Article cannot be met, operators of essential services, in accordance with risk assessment, shall:
– implement the measures reducing residual risk that occurred due to inability of limited hardware and software use and necessary data traffic
– record and accept residual risks.
(3) Rules defining data traffic limitations, such as network addresses, protocols and ports, shall be regularly updated in accordance with the functional and security requirements of the essential system.
(4) Data traffic limitations shall be implemented within the essential system, between functional subsystems, as well as in external connections of the essential system.
(5) Essential system configuration and the list of all elements comprising the essential system shall be recorded in detail.

Preventive essential system vulnerability assessment
Article 31

(1) Operators of essential services shall, in accordance with risk assessment, ensure the implementation of regular and continuous vulnerability assessment of essential systems, especially those system parts that use the resources on publicly available network and information systems.
(2) Operators of essential services shall ensure that the defects and vulnerabilities identified during vulnerability assessment and penetration testing are processed through risk management procedure.

Business continuity management
Article 32

(1) Operators of essential services shall identify business processes necessary to ensure business continuity of essential service in cases of incidents referred to in Article 35 of this Regulation.
(2) Operators of essential services shall adopt operative plans with the aim of ensuring business continuity of essential services, which shall include at least:
– specific technical procedures for essential service recovery
– clear steps and responsibilities for activating essential service recovery plans
– defined timeframes for the recovery of essential service.
(3) Operators of essential services shall, in accordance with risk assessment, periodically perform and record the testing of plans referred to in paragraph 2 of this Article
.

Backup storage
Article 33

(1) Operators of essential services shall establish the process of backup storage management for the information necessary in order to reestablish essential services within the predefined timeframe.
(2) Backup storage management process shall include the process of creating, storing and testing backup copies and recovering information from backups.
(3) Backup copies shall be updated and stored in one or more locations, at least one of which, in accordance with risk assessment, is adequately remote from the original location.

PART III
INCIDENT NOTIFICATION

CHAPTER I
MANDATORY INCIDENT NOTIFICATION

Responsibility for notification
Article 34

Operators of essential services and digital service providers shall, without undue delay, notify the competent CSIRT about incidents that have a significant impact on the continuity of services they provide.

Incidents with significant impact on the continuity of providing essential service
Article 35

(1) The incident's impact on the continuity of providing essential service shall be determined in accordance with the following criteria:
– number of users affected by disruption of essential service provision
– duration of incident
– geographical spread of incident or
– other sectoral criteria such as economic impact and dependency of other fields or activities on service provision.
(2) Incidents with significant impact on the continuity of providing essential service are the incidents that meet the criteria referred to in paragraph 1 of this Article, divided by essential services and incidents in accordance with the List in Appendix I of this Regulation, which forms the integral part of this Regulation.

Incidents with significant impact on the continuity of providing digital service
Article 36

Incidents with significant impact on the continuity of providing digital service are incidents that meet the criteria referred to in Article 4 of the Commission Implementing Regulation.

Incident's impact assessment on the continuity of providing essential service
Article 37

(1) Operators of essential services shall ensure the implementation of impact assessment of all incidents in order to identify incidents with significant impact on the continuity of providing essential service.
(2) Operators of essential services shall ensure the implementation of the assessment referred to in paragraph 1 of this Article in a way that:
– number od users affected by the disruption in providing essential service may be identified according to the number of individuals and legal entities to which the operator of essential service is obliged to provide the service pursuant to regulation or legal arrangement or, if due to specific circumstances of an incident this does not apply, the number of individuals and legal entities using the service assessed on the basis of information on essential service use from the previous period
– incident duration may be identified according to duration of service termination or disruption of service provision affecting its availability, authenticity, integrity or confidentiality
– geographical spread of incident may be identified according to the size of area where users of essential service were affected by its termination, including the areas in other member states.
(3) In the case where it cannot be identified when the time of service termination or disruption started, incident duration shall be identified in accordance with the duration of termination or service disruption from the moment when the termination or disruption was discovered.
(4) Operators of essential services shall perform the assessment referred to in paragraph 1 of this Article continuously during the entire incident duration, while the incident is not handled.

Incident's impact assessment on the continuity of providing digital service
Article 38

Digital service providers shall ensure the implementation of impact assessment of all incidents in order to identify incidents with significant impact on the continuity of providing digital service in

accordance with the parameters stipulated for such purpose by the Commission Implementing Regulation.

CHAPTER II
SECTION A

NOTIFICATIONS ABOUT INCIDENTS WITH SIGNIFICANT IMPACT ON THE CONTINUITY OF SERVICE PROVISION

Notification types
Article 39

Operators of essential services and digital service providers shall provide the following notifications about incidents with significant impact on the continuity of service provision (hereinafter referred to as: incidents with significant impact):
– initial notification about incident with significant impact
– interim report about incident with significant impact and
– final report about incident with significant impact.

Initial notification about incident with significant impact
Article 40

(1) Initial notification about incident with significant impact shall be provided immediately, and at latest four hours from the moment the incident with significant impact was discovered.
(2) Initial notification about incident with significant impact shall include the description of incident's basic features and its expected consequences, based on the information available to the operator of essential service or digital service provider during impact assessment and after discovering the incident with significant impact.
(3) Initial notification about incident with significant impact shall also include the estimated day of providing the transitional report about incident with significant impact, which cannot be later than three working days from the day of submitting the initial notification about the incident.

Interim report about incident with significant impact
Article 41

(1) First interim report about incident with significant impact shall be provided within three working days the latest from submitting the initial notification about incident.
(2) First interim report about incident with significant impact shall include a detailed description of incident and its consequences.
(3) If all relevant data is not available, operators of essential services and digital service providers shall submit the first interim report with a note that the descriptions are based on information assessment.
(4) Operators of essential services and digital service providers shall, without delay, submit the additional interim reports about incidents with significant impact if new information becomes known or significant changes occurred since the first interim report, especially if the incident escalated or reduced or new causes were discovered or new actions for incident handling have been implemented.

Final report about incident with significant impact
Article 42

(1) Operators of essential services and digital service providers shall submit the final report about incident with significant impact at latest within 15 days since the day it was estimated that the regular service provision was reestablished.
(2) Final report about incident with significant impact shall include the real information about the incident's impact, analysis of incident causes, summary of measures implemented in order to mitigate the incident or that are planned to be implemented in order to remove the noticed vulnerability and prevention of future incidents.
(3) Operators of essential services and digital service providers shall submit the final report about incident with significant impact even before the expiry of deadline referred to in paragraph 1 of this Article if they establish that the already reported incident does not meet the criteria for identifying incidents with significant impact and it is not expected that the criteria will be met before the incident is handled, where the competent CSIRT shall be notified immediately.
(4) Notification referred to in paragraph 3 of this Article shall include the indication of the final report submission date.
(5) Operators of essential services and digital service providers shall notify the competent CSIRT about the extension of deadline referred to in paragraphs 1 and 4 of this Article, if the real information about incident’s impact are not available.
(6) The notification referred to in paragraph 5 of this Article shall include the explanation of delay and the new estimated deadline for submitting the final report, which cannot be longer than 30 days since the day it was estimated that the regular service provision was reestablished.

Submitting the notification about incidents with significant impact
Article 43

(1) Competent CSIRT shall adopt guidelines for submitting the notification about incidents with significant impact, which shall define the means of submitting the notification and the forms for mandatory notification about incidents with significant impact.
(2) Competent CSIRT shall define the forms referred to in paragraph 1 of this Article with the consent of the competent sectoral authority.
(3) Operators of essential services and digital service providers shall submit the notifications about incidents with significant impact in accordance with the guidelines referred to in paragraph 1 of this Article.

Exchange of notifications
Article 44

(1) Competent CSIRT shall immediately forward the received notifications about incidents with significant impact to the competent sectoral authority.
(2) Notwithstanding the provisions of paragraph 1 of this Article, competent CSIRT is not obliged to forward the received notifications about incidents with significant impact if the competent sectoral authority, pursuant to special regulation, receives incident notifications directly from operators of essential services, which fulfill the requirements from the Act and this Regulation in terms of their content and objective.
(3) Competent sectoral authority shall notify the competent CSIRT about the exceptions referred to in paragraph of this Article.

SECTION B

PROCEDURE FOLLOWING THE NOTIFICATIONS ABOUT INCIDENTS WITH SIGNIFICANT IMPACT

Handling incidents with significant impact
Article 45

(1) Competent CSIRT, after receiving the request of the operator of essential services, digital service provider or competent sectoral authority for handling incidents, shall analyze and classify incidents on the basis of received notifications about incidents with significant impact and shall participate in the incident handling procedure.
(2) Competent CSIRT, while handling incidents with significant impact, may use the expert assistance of the national CSIRT competent for another sector, CSIRTs of other member states competent for the sector where the incident occurred and, when necessary, European Commission CSIRT network.
(3) Competent CSIRT shall, in cooperation with the competent sectoral authority, determine the cross border effect for any incident with significant impact.
(4) Competent sectoral authority shall assess the impact of each individual incident, which was notified in accordance with paragraph 44 of this Regulation, on the continuity of providing essential or digital service at sectoral level.
(5) Competent sectoral authority shall, based on the assessment referred to in paragraph 4 of this Article, participate in the procedure of establishing service continuity, when the continuity of providing essential or digital service is adversely affected at sectoral level.

Records of incidents with significant impact
Article 46

(1) Competent CSIRTs shall keep records of all incidents with significant impact by sectors and subsectors from the Appendix I of the Act.
(2) Records referred to in paragraph 1 of this Article and deadlines for submitting the information from records to the single national point of contact shall be defined by the guidelines adopted by the single national point of contact.

CHAPTER III
VOLUNTARY INCIDENT NOTIFICATION

Article 47

(1) Entities providing essential services from the List in Appendix I of the Act or digital services from the List in Appendix II of the Act, which do not represent an operator of essential services or digital service provider within the scope of this Regulation, may notify the competent CSIRT about incidents which caused termination or significant disruption in the provision of essential or digital service.
(2) Entities referred to in paragraph 1 of this Article shall submit the notifications about incidents on voluntary basis in accordance with the guidelines referred to in Article 43 of this Regulation.

(3) Competent CSIRT shall act upon request to handle incidents referred to in paragraph 1 of this Article in accordance with the priorities and available resources, taking into consideration the requirements referred to in Article 45 of this Regulation.

PART IV
TRANSITIONAL AND FINAL PROVISIONS

Article 48

Competent CSIRTs shall adopt the guidelines referred to in Article 43, paragraph 1 of this Regulation within 90 days from the day this Regulation enters into force.

Article 49

This Regulation shall enter into force 8 days following its publication in the Official Gazette.
Class: 022-03/18-03/34
Reg. No: 50301-29/09-18-8
Zagreb, 26 July 2018.

President
Andrej Plenković, m. p.

APPENDIX I
CRITERIA FOR DETERMINING THE INCIDENTS WITH SIGNIFICANT IMPACT ON ESSENTIAL SERVICE PROVISION

Sector	Subsector	Essential service	Criteria	Thresholds
Energy	Electricity	Production of electricity	Production decrease	60 MW
		Transmission of electricity	Transmission interruption	No exception
		Distribution of electricity	Electricity supply interruption	More than 20 000 metering points
	Oil	Oil transmission pipelines	Transmission interruption	No exception
		Oil production	Oil field production decrease	10 000 tons per year
		Production of petroleum products	Petroleum products production decrease	Motor gasoline: 40 000 tons per year Diesel fuel: 40 000 tons per year Gas oils: 20 000 tons per year
		Storage of oil and petroleum products	Decrease of oil storage capacity in a terminal	200 000 m^3
			Decrease of storage capacity in a single storage of petroleum products	12 000 m^3
	Gas	Distribution of gas	Interruption of distribution to end users	More than 20 000 metering points
		Transport of gas	Transport interruption	No exception
		Storage of gas	Decrease of storage capacities	5 % of gas consumption in the Republic of Croatia in the previous year
		LNG importation and offloading	Decrease of LNG regasification capacity in m3/h	More than 100 000 m3/h
		Production of natural gas	Decrease of gas production transmitted	20%

			to the transport system at individual entry	
Transport	Air transport	Air transport of passengers and cargo	Number of incident affected passengers in a single airport	20% from average traffic
		Managing airport infrastructure, including ancillary installations contained within airports	Number of incident affected passengers in a single airport	20% from average traffic
		Air traffic control	Disruption of integrity of information in essential operating systems	1 aircraft affected in any volume of controlled airspace and in airport maneuvering areas
			Loss of information in essential operating systems	1 aircraft affected in any volume of controlled airspace and in airport maneuvering areas
	Rail transport	Managing and maintaining rail infrastructure, including traffic management and control-command and signal-security subsystem	Disruption of integrity of traffic management, signal-security or electrical-energy subsystem	No exception
		Rail transport services of goods and/or passengers	Number of units (trains) affected by incident	10 per day
		Managing service facilities and providing services in service facilities	Number of units (trains) affected by incident	10 per day
		Providing additional services necessary for rail transport of goods or passengers	Number of units (trains) affected by incident	10 per day

	Water transport	Maritime traffic monitoring (VTS service)	Disruption of integrity of maritime traffic monitoring and management system (VTMIS) and VTS service provision	Disabled use of full functionality of maritime traffic monitoring and management system (VTMIS) and VTS service provision from at least one control center for more than 3 hours
		Maritime radio services	Disruption of integrity of maritime radio service system and maritime radio service system provision	Disabled use of full functionality of maritime radio service system and maritime radio service system provision from at least one coastal radio station for more than 3 hours
		Managing maritime signaling facilities	Disruption of integrity of maritime signaling facilities of 1st navigation security category	Unavailability of at least 20% of maritime signaling facilities of 1st navigation security category in a single navigation area for more than 3 hours
				Unavailability of at least 20% of maritime signaling facilities of 1st navigation security category in ports open for public traffic with special (international) economic significance for the Republic of

				Croatia with access waterways for more than 3 hours
		International and/or domestic passenger transport	Other sectors' dependency on the service	All sectors whose users or employees use maritime transport
			Incident impact on economic and societal activities and public safety	Incident duration of more than one day
		Cargo loading and offloading in ports in international and domestic traffic	Operating system unavailable and restricted	Inability to perform port operations for a period longer than 3 days
			Importance of maintaining the sufficient service level	If incident causes inability to perform essential service for a period longer than 3 days it may cause deadlocks in dependent sectors
			Importance of maintaining the sufficient service level	If incident causes inability to perform essential service for a period longer than 3 days it may cause deadlocks in dependent sectors
		Transport of passengers, cargo and vehicles in inland maritime waters and territorial sea of the Republic of Croatia on previously	Disabled transport service provision	Interruption of transport service on more than 30% of the lines for more than 3 hours

		defined lines according to public journey schedule and price list		
		Tracking and locating vessels in inland waterways	Disabling RIS system work which relates to tracking and locating vessels in inland waterways	Threat to tracking and locating at least on vessel in inland waterways
		Notifications to vessels in inland waterways	Disabling accurate and timely notification to vessels in inland waterways	Threat to minimum one notification to vessels in inland waterways
		Access to electronic navigation charts in inland waterways	Disabling the work of user workstations on the coast in access to electronic navigation charts in inland waterways (ENC)	Disabled usage of minimum one ENC cell
		Hull data base in inland waterways	Threat to content accuracy in data base	Threat to content accuracy in data base for minimum one vessel
		Electronic reporting international in inland waterways	Inability to send and receivce ERI messages	Inability to send/receivce minimum one ERI message
	Road transport	Public passenger transport	Number of transport units affected by incident	20
			Number of passengers affected by incident	10 000
		Road infrastructure usage	Threats to integrity of traffic-management, electrical-energy or fire protection system in road infrastructure (including: bridges, tunnels, viaducts)	No exception

		Traffic flow management or intelligent transport systems (ITS)	Service interruption in traffic management and control center	30 minutes
			Service interruption in center for informing the drivers on traffic situation	60 minutes
			Number of traffic lights affected by incident	10
Banking		Payment services	Criteria that operators of essential services in banking sector shall use to classify major operative or security incidents according to European Banking Authority (EBA) guidelines from Article 96, paragraph 3 of Directive (EU) 2015/2366 on payment services in the internal market (PSD2 Directive)	Thresholds that operators of essential services in banking sector shall use to classify major operative or security incidents according to European Banking Authority (EBA) guidelines from Article 96, paragraph 3 of PSD2 Directive
Financial market infrastructure		Trading venue services	Incident duration	30 minutes
		Central counterparties services (CCP)	Incident duration	30 minutes
Health sector		Primary health care	Unavailability of Croatian central health information system	8 hours
			Unavailability of Health VPN network HealthNet	8 hours
			Unavailability of approved program solution for health care provider	12 hours

			Unavailability of emergency medical information system	8 sati
		Secondary health care	Unavailability of Croatian central health information system	8 hours
			Unavailability of Health VPN network HealthNet	8 hours
			Unavailability of approved program solution for health care provider	12 hours
			Unavailability of hospital information system in general hospital	1 hour
		Tertiary health care	Unavailability of Croatian central health information system	8 hours
			Unavailability of Health VPN network HealthNet	8 hours
			Unavailability of hospital information system in clinical hospital center	1 hour
			Unavailability of hospital information system in clinical hospital	1 hour
			Unavailability of hospital information system in clinic	1 hour
		Transfusion medicine and organ transplantation	Unavailability of information system for transfusion medicine	8 hours
			Unavailability of Health VPN network HealthNet	8 hours
			Unavailability of the coordinator of National organ transplantation program	1 hour

		Health insurance and cross border health care	Unavailability of ZOROH information system – Health insurance – registry of insured persons in Croatia	24 hours
			Unavailability of service to check status of compulsory and supplemental health insurance	8 hours
			Unavailability of system for issuance of European Health Insurance Cards	72 hours
		Food safety	Unavailability of Central information system of the sanitary inspection	24 hours
		Protection against hazardous chemicals	Unavailability of Safety Data Sheet Registry	72 hours
			Unavailability of Registry of hazardous chemicals produced or imported on the territory of the Republic of Croatia	72 hours
		Distribution and security of medicines and medical products	Inability to stop placing on the market or withdraw medicines from the market	72 hours
			Inability to monitor serious non-compliance and quality tests of medicines on the market in the Republic of Croatia	60 hours
			Inability to monitor medical products' security	84 hours
		Control over health care status of the population and human resources in health care by	Unavailability of National public health care information system	8 hours
			Unavailability of Health VPN network HealthNet	8 hours

		managing public health care registries		
Drinking water supply and distribution		End users' supply	Supply interruption of safe water from public water supply system	more than 24 hours
			Total interruption of water supply from public water supply system	more than 24 hours
Digital infrastructure		DNS service for .hr TLD	Service unavailability	60 min
			Unauthorized change of information on domains	20% of total number of registered.hr domains
		Domain name registry for .hr TLD	Service unavailability	180 min
			Unauthorized change of information on domains	20% of total number of registered.hr domains
		System for registration and administration of secondary domain	Service unavailability	180 min
			Unavailability of authorized registries	40% of total registries
		IXP service	Service unavailability for 50% members connected	8 hours
			Service unavailability for 75% members connected	4 hours
			Service unavailability for all members connected	2 hours
Business services for state authorities		Services in e-citizen system	Number of users affected by interruption	20%
			Incident duration	2 hours
		Business services for state budget users	Incident duration	1 hour
			Number of sectoral users affected by incident	1