CROATIAN REGULATORY AUTHORITY FOR NETWORK INDUSTRIES

Pursuant to Article 12(1) (1), Article 19(1) and Article 99(9) of the Electronic Communications Act (Official Gazette 73/08, 90/11, 133/12, 80/13, 71/14 and 72/17), the Council of the Croatian Regulatory Authority for Network Industries adopts

ORDINANCE ON
THE MANNER AND DEADLINES FOR THE
IMPLEMENTATION OF MEASURES FOR PROTECTING
SAFETY AND INTEGRITY OF NETWORKS AND SERVICES

GENERAL PROVISIONS

CONTENTS OF THE ORDINANCE

Article 1

This Ordinance lays down the manner and deadlines for providers of electronic communications networks or publicly available electronic communications services (hereinafter: providers) to take all appropriate measures to ensure the security and integrity of their networks, with a view to ensuring the continuous performance of the services provided through those networks, and regulates the manner in which the Croatian Regulatory Authority for Network Industries (hereinafter: the Agency) is informed of a breach of security and/or loss of integrity which has a significant impact on the operation of their networks or the provision of their services.

TERMS AND DEFINITIONS

Article 2

For the purposes of this Ordinance, individual terms shall have the following meanings:

1. *network integrity*: a set of technical requirements for processes, operation and modifications in the electronic communications network, with a view to ensuring continuity of interconnected electronic communications networks, as well as access to those networks and the integrity of data stored in the electronic communications network,

2. ENISA European Union Agency for Network and Information Security: European Union Agency for Network and information Security,

3. *ICT product*, process or service: meaning as laid down in Regulation (EU) 2019/881

4. *information system*: communication, computer or other electronic system used for processing, storing or transmitting data, with a view to making it accessible and useful to the authorised users,

5. *National taxonomy for computer security incidents*: uniform criteria for classifying cyber security incidents in its own information and network systems, at the national level

6. *National CERT:* National body for prevention and cyber threat protection of the security of public information systems in the Republic of Croatia,

7. *Pixi platform*: National platform for collecting, analysing and exchanging information on cyber security threats and incidents and reporting significant cyber-security incidents,

8. *Security policy*: a set of rules, guidelines and procedures defining how to make the information system secure and how to protect its values, including hardware, software and data;

9. *security incident*: an event that has a real negative impact on the security of electronic communications networks or services;

10. *security of networks and services*: the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or related services offered by or accessible via those electronic communications networks or services,

11. *impact on authenticity*: compromising users identity,

12. impact on integrity: intentionally or accidentally unauthorized alteration of communication data or metadata;

13. *impact on availability:* impact on continuity of service provision, degradation of service performance, and partial or full failure of network or service,

14. *impact on confidentiality*: compromising the confidentiality of communication, communication data or metadata;

15. *significant cyber security incident*: a cyber security incident affecting critical data (unclassified and classified) and/or information systems and computer networks in the public and private sectors, especially systems that are part of the national critical infrastructure, on which these data are processed and transferred, and which can have or has negative impact on the everyday life of a large number of citizens, the national economy and national security as a whole.

MEASURES FOR PROTECTING OF SECURITY AND INTEGRITY OF NETWORKS AND SERVICES

General obligations

Article 3

(1) Providers shall take appropriate technical and organisational measures, including encryption, where appropriate, to protect the security and integrity of their networks and services and to prevent and mitigate the impact of security incidents on users and interconnected electronic communications networks and services, whereby the measures taken shall ensure a level of security corresponding to the existing level of risk to the safety of networks and services.

(2) Technical and organisational measures referred to in paragraph 1 of this Article include in particular:

- governance and risk management including security policy and it's based on a risk assessment, with appropriate application of the relevant ENISA technical guidelines on threats;
- human resources security
- security of systems and facilities
- operations management
- incident management
- business continuity management
- monitoring and security testing
- threat awareness.

(3) When implementing the measures referred to in paragraphs 1 and 2 of this Article, providers shall, to the maximum extent possible, apply the relevant ENISA technical guidelines on security measures, threats and other relevant guidelines.

(4) A list of reference standards for the implementation of measures referred to in paragraphs 1 and 2 of this Article is provided in Annex 1 to the Ordinance.

(5) In addition to the reference standards referred to in Annex 1 to the Ordinance, providers may also apply other relevant standards and relevant national and/or international security standards for the purpose of achieving the measures specified in this Ordinance.

(6) The measures referred to in paragraph 2 of this Article shall ensure the application of security policy in the processing and protection of personal data.

(7) Providers shall document taken and implemented measures specified in paragraphs 2 and 6 of this Article and make them available to the Agency upon request.

(8) Providers with more than 100 000 users shall submit to the Agency, by electronic means once a year at the latest by the end of January, a security policy for the previous year covering the measures specified in Annex 1 and Article 4 of this Ordinance, and at the request of the Agency also several times during the year. Providers with less than 100 000 users shall submit to the Agency a security policy upon request.

Security of 5G networks and services

Article 4

(1) With regard to 5G networks, the security policy shall also contain a list of critical network components and sensitive parts of the 5G network, taking into account the list of critical and sensitive parts of the 5G network defined by the document EU Coordinated Risk Assessment on Cybersecurity in 5G Networks.

(2) In addition to the measures specified in Article 3, paragraph 2 of this Ordinance, 5G providers shall implement the following additional technical and organizational measures:

- equipment for critical and sensitive parts of the 5G network must comply with relevant 5G standards, in particular 3GPP standards in accordance with relevant ENISA guidelines, as well as applicable EU and national programmes (certification schemes) on cyber security

- 5G equipment supply security system, including, among other things, a security assessment of all contracted contractors, manufacturers and their suppliers, and supervision system of the manner and quality of provision of contracted tasks and services with appropriate application of relevant ENISA guidelines regarding the procurement of safe ICT processes, products and services;

- use of suppliers demonstrating an appropriate level of long-term viability/resilience of equipment and/or ICT processes, products and services

- carrying out security controls in accordance with the relevant standards for 5G networks and service security

- restriction and control system of third parties remote access to the critical part of the network and information system and the implementation, where possible, of the principle of least privileged and division of tasks

- Network Operation Centre (NOC) and Security Operations Centre (SOC) must be located in the territory of one of the EU Member States

- NOC and SOC, each within their scope of work, must monitor critical network components and sensitive parts of 5G networks for the purpose of timely detecting irregularities and detecting and preventing threats

- communication networks or services traffic management protection measures in order to prevent unauthorised changes to network or service components;

- MEC (Multi-Access edge computing) and base stations physical protection measures based on risk assessment, for example where components are deployed and used, and specific access measures for a limited number of security-verified, qualified staff with limited and supervised access by third parties

- tools and processes to ensure software integrity when updating and applying security patches, reliable identification and monitoring of changes and patch status, especially in virtualised network functions

- recovery procedures for incidents that also affect interdependent critical sectors and services.

(3) When implementing measures referred to in paragraph 2 of this Article, providers shall, to the maximum extent possible, apply the relevant ENISA technical guidelines on 5G network security measures.

(4) Providers shall document the measures referred to in paragraph 2 of this Article.

A Network and Services Security Audit

Article 5

(1) At least once a year the providers shall carry out network and services risk assessment and security audit in order to determine whether the minimum security measures laid down in Annex 1 and Article 4 of this Ordinance have been met, taking into account the results of previous audits.

(2) Audit may be performed by provider’s employees who are not related to the auditing area and who have an adequate knowledge and experience or an external audit body.

(3) Providers with more than 100 000 users shall submit the findings of the audit referred to in paragraph 1 of this Article as well as the plan for removing of detected deficiencies to the Agency by 30 May of the current year for the previous year. Providers with less than 100 000 users shall submit an audit finding to the Agency at its request.

(4) The Agency may impose additional measures on providers if it deems a plan for removing of detected deficiencies referred to in paragraph 3 of this Article not appropriate for prevention and mitigation of the security and cyber-security incidents impact on users and interconnected electronic communications networks or to ensure the integrity of networks and services.

(5) The Agency may adopt binding instructions, including the possibility for issuing orders to providers to take measures to prevent a security incident when a significant threat is identified and/or in order to resolve a security incident and implementation deadlines.

(6) Regardless of the audit findings, the Agency may impose measures on providers to ensure the security and integrity of electronic communications networks and services, in particular 5G networks, in case it finds it necessary for reasons of national security, on the basis of the prior opinion of the competent national security authority or to ensure essential services defined by the relevant Act, upon the proposal of competent authorities.

NOTIFYING SECURITY INCIDENTS TO THE AGENCY

Article 6

(1) Providers shall notify the Agency of a security incident that has significant impact on the operation of networks and/or services in accordance with the reporting criteria set out in Annex 2, whereby providers shall verify the fulfilment of the quantitative criteria and, if they are not satisfied, verify the

fulfilment of the qualitative criteria set out in that Annex. In case of each security incident, providers shall always verify whether there has been a significant computer security incident in accordance with the National taxonomy for computer security incidents referred to in that Annex.

(2) In case of failure of at least one of two redundant cables/information systems, providers shall report this security incident as an incident that has an impact on redundancy by applying the template from Annex 3 of this Ordinance accordingly.

(3) The notification of safety incidents referred to in paragraph 1 of this Article shall be submitted to the Agency without delay, as soon as the information is available, by means of the template prescribed in Annex 3 to this Ordinance:

1. within a maximum period of 1 hour from the fulfilment of the reporting criteria, i.e. the expiry of the minimum duration of the security incident referred to in Annex 2,

2. within a maximum period of 1 hour from the elimination of the security incident,

3. within a maximum period of 20 days from the date of elimination of the security incident.

(4) In the event of a security incident that meets quantitative or qualitative criteria for reporting and at the same time that security incident is a significant cyber security incident in accordance with the National taxonomy for computer security incidents referred to in Annex 2, providers shall submit to the Agency a notification of the incident through the template from Annex 3 of this Ordinance and via the Pixi platform. Additional obligations for reporting significant cyber security incidents are laid down in Article 7 of this Ordinance.

(5) Providers shall provide the Agency with contact details in accordance with Annex 3 of this Ordinance for the purpose of quick exchange of information on security incidents, as well as to provide the necessary technical information to the Agency in order to monitor the security and integrity of public communications networks.

(6) All notifications of security incidents shall be submitted to the Agency using a secure data transfer protocol or in an encrypted form by electronic means to an e-mail address incidenti@hakom.hr or otherwise appropriate in accordance with the form referred to in Annex 3 to this Ordinance.

(7) The Agency may request amendments to the report referred to in paragraph 2 for the purpose of monitoring a specific security incident and a better understanding of the nature of the occurred security incident.

(8) Providers may also inform the Agency of other, in their opinion, important security incidents referring to the safety and integrity of public communications networks and/or services not covered by the security incidents referred to in paragraph 1 of this Article.

ADDITIONAL OBLIGATIONS FOR SIGNIFICANT COMPUTER SECURITY INCIDENTS

Article 7

(1) Notification of significant cyber security incidents in accordance with the National taxonomy for computer-security incidents shall be submitted via the Pixi platform. Conditions and manner of using this platform are prescribed by the Conditions of use of the Pixi platform on the National CERT website.

(2) After considering the reported incidents, the Agency shall, in cooperation with the national CERT, order any updates to the report and take other measures to prevent or eliminate incidents, including the provision of specific recommendations, guidelines and warnings on security threats.

(3) In case of the need to initiate an appropriate procedure within the competence of the Agency in reference to the reported incidents, the Agency shall actively cooperate with the national CERT and, if necessary, request expert assistance and coordination in defining specific activities and corrective actions related to resulting or potential cyber security incidents.

NOTIFYING OTHER ENTITIES ABOUT SECURITY INCIDENTS

Article 8

Providers shall without delay:

1. Inform their users in a clear and easily demonstrable manner about a security incident that has significantly affected the operation of public communications networks and/or services, in accordance with the reporting criteria in Annex 2 and publish information on the significant incident on its official website. Information on a significant incident must include a description of the area covered by the incident, which may also be shown in cartographic form.

2. In the event of a particular danger of a security incident in public electronic communications networks or publicly available electronic communications services, inform their users potentially affected by such danger, of the measures available to eliminate the danger and / or its consequences and, if appropriate, of the security threat.

FINAL PROVISIONS

Article 9

1. The Ordinance on the manner and deadlines for the implementation of security measures and the integrity of networks and services ceases to apply (OG 109/12, 33/13-correction, 126/13, 67/16 and 66/19) with the entry into force of this Ordinance.

2. This Ordinance shall enter into force 30 days from the date of its publication in the Official Gazette, except for Article 4 which shall enter into force on 1 June 2022.

CLASS: 011-02/21-02/10

REG. NO. : 376-05-4-21-

Zagreb, 14 October 2021.

CHAIRMAN OF THE COUNCIL

Tonko Obuljen

ANNEX 1

MINIMUM SECURITY MEASURES

Minimum security measures	Referential norms
Governance and risk management	ISO 27001:2013 ISO 27002:2013 ISO 27005:2018 ISO 27036-3:2013
Human resources security	ISO 27001:2013 ISO 27002:2013
Security of systems and facilities	ISO 27001:2013 ISO 27002:2013
Operations management	ISO 27001:2013 ISO 27002:2013
Incident management	ISO 27001:2013 ISO 27002:2013
Business continuity management	ISO 27001:2013 ISO 27002:2013 ISO 22301:2019
Monitoring and security testing	ISO 27001:2013 ISO 27002:2013
Threat awareness	ISO 27001:2013 ISO 27002:2013

ANNEX 2

QUANTITATIVE TRESHOLDS

A security incident affects: **fixed telephony/mobile telephony/fixed internet access,/ mobile internet access,/number independent interpersonal communications service/machine-to-machine (M2M)/broadcasting**	**Number of users affected by security incident[1]**	**Duration of the security incident**
Availability	1% - 2%	8 hours
Availability	2% - 5%	6 hours
Availability	5% - 10%	4 hours
Availability	10% - 15%	2 hours
Availability	> 15%	1 hour
Availability	> 1 000 000 user/hours	
Confidentiality / authenticity / integrity	> 1%	Regardless of duration

[1] The data is obtained by dividing the number of users covered by the incident with the total number of users of a particular service in Croatia (annual data are available on the Agency's website) and dividing result with 100.

QUALITATIVE TRESHOLDS

Security incident	**availability/confidentiality/ authenticity/integrity**
1. Significant due to the geographical spread of the incident (cross-border, or if large remote/rural areas or , islands, or a capital city of Zagreb are affected, etc.) 2. Significant due to the impact on the economy and society or on users (lack of access to 112, national emergency numbers, impact on public warning systems, high material damage, high risks to public safety or loss of life, media coverage, impact on the continuity of essential services or critical sectors/operators, impact on a specific days such as election or referendum days).	regardless of duration and number of affected users

ANNEX 3

TEMPLATE FOR REPORTING A SECURITY INCIDENT

Necessary data	**Completed by the operator**
Operator	
Date of submitting the report	
Time and date of occurrence/ discovery of security incident	
Incident description	
Type of incident	☐ A - Service outage (e.g. continuity, availability) ☐ B - Other impact on services (e.g. confidentiality, integrity, authenticity) ☐ C - Impact on other systems (e.g. ransomware) an office network, without affecting the service) ☐ D - Threat or vulnerability (e.g. discovery of crypto flaw) ☐ E - Impact on redundancy (e.g. failover or backup system) ☐ F - Near-miss incident (e.g. activation of security measures)

Services impacted	☐ Fixed telephony		Number of users		Duration
	☐ Mobile telephony		Number of users		Duration
	☐ Fixed Internet		Number of users		Duration
	☐ Mobile Internet		Number of users		Duration
	☐ OTT services		Number of users		Duration
	☐ M2M		Number of users		Duration
	☐Broadcasting		Number of users		Duration
	☐ Other		Number of users		Duration

Root cause category	☐ System failures ☐ Human errors ☐ Malicious action ☐ Natural phenomena ☐ Third party failures
Service and subservice technology	☐ Cable ☐ DSL ☐ Email ☐ Fiber ☐ GRPS/EDGE ☐ GSM ☐ Instant messaging protocol ☐ LTE ☐ MTC ☐ PSTN ☐ Signal Protocol ☐ UMTS ☐ URLLC ☐ VoIP ☐ Web/App ☐ eMBB ☐ Other
Technical causes	☐ Arson ☐ Cable cut ☐ Cable theft ☐ Cooling outage ☐ DDoS attack ☐ Earthquake ☐Eavesdropping ☐ Electromagnetic interference ☐ External environmental causes ☐Faultyhardware change/update ☐ Faulty software change/update ☐ Fire ☐ Flood ☐ Fuel exaustion ☐ Hardware failure ☐ Hardware theft ☐ Heavy snow/ice ☐ Heavy wind ☐ Identity theft ☐ Malware and viruses ☐ Network traffic hijack ☐ Overload ☐ Phishing ☐ Policy/procedure flaw ☐ Power cut ☐ Power surges ☐ Security shutdown ☐ Software bug ☐ Vulnerability exploit ☐ Wildfire ☐ Other

Technical assets affected	☐ Addressing Servers ☐ App ☐ Backup power supplies ☐ Billing and mediation system ☐ Buildings and physical security system ☐ Cloud storage ☐ Cooling system ☐ Inteligent network devices ☐ Interconnection points ☐ Logical security system ☐ Mobile base stations and controllers ☐ Mobile messaging center ☐ Mobile switches ☐ Mobile user and location registers ☐ Operational support systems ☐ Overhead cables ☐ PSTN switches ☐ Power supplies ☐ SIM/eSIM ☐ Street cabinets ☐ Submarine cables ☐ Subscriber quipment ☐ Switches and routers ☐ Transmission nodes ☐ Underground cables ☐ website ☐ Other
Significance factors	☐ Number of users affected ☐ Duration of the incident ☐ Geographical spread ☐ Extent of disruption on functioning ☐ Impact on the economy and society
Scale of impact	☐ No impact ☐ Minor impact ☐ Large impact ☐ Very large impact
Threat severity factors (for Type D)	☐ Mitigatinon costs ☐ Potential damage ☐ Rate of spreading of the threat ☐ Likehood of exposure ☐ Criticality of systems potentially affected ☐ Lack of good solutions to mitigate the threat
Severity of threat	☐ Small ☐ Medium ☐ High

Rsolving the security incident and a description of the measures taken	
Measures taken after the removal of a security incident	
Long-term measures	
Contact data for process monitoring	
Other important information	