GOVERNMENT OF THE REPUBLIC OF CROATIA

Pursuant to Article 24 of the Cybersecurity Act (Official Gazette, No 14/24), the Government of the Republic of Croatia, at its session held on 21 November 2024, adopted the

REGULATION

ON CYBERSECURITY

PART ONE
GENERAL PROVISIONS

Article 1

This Regulation defines the benchmarks for the classification of entities based on special entity categorisation criteria, criteria for assessments conducted to categorise public sector and education system entities, collecting data for categorisation of entities and for maintaining a special registry of entities, maintaining a list of essential and important entities, maintaining a special registry of entities, cybersecurity risk-management measures and the manner of their implementation, conducting of cybersecurity self-assessments, statement of compliance form, criteria for identifying significant incidents, notification of significant incidents, other incidents, cyber threats and near misses, access rights and other issues relevant for the use of the national platform for the collection, analysis and exchange of data on cyber threats and incidents, submission of requests and proposals, collection of data necessary for assessing the criticality of entities, as well as other issues relevant for the implementation of the access of entities to the national system for detecting cyber threats and protecting cyberspace.

Article 2

An integral part of this Regulation are:

- Annex I – List of Activity Sectors (hereinafter: Annex I to this Regulation)
- Annex II – Cybersecurity Risk-Management Measures (hereinafter: Annex II to this Regulation)
- Annex III – Specific Physical Security Measures for Digital Infrastructure Sector Entities (hereinafter: Annex III to this Regulation), and
- Annex IV – Statement of Compliance Form (hereinafter: Annex IV to this Regulation).

Article 3

This Regulation transposes into Croatian law Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333/80, 27.12.2022).

Article 4

(1) For the purposes of this Regulation, the following definitions apply:

1. *activity* is any activity explicitly listed in Annexes I and II to the Cybersecurity Act (Official Gazette, No 14/24; hereinafter: the Act)
2. *hacktivism* implies the use of cyberattacks to promote and encourage certain political views or social changes, as well as to express some form of civil disobedience, carried out by organised cyber groups or individuals called hacktivists
3. *indicators of compromise (IoCs)* are data that represent indicators of a possible compromise of a network and information system, which are used to detect and prevent cyberattacks, i.e. to mitigate potential damage by stopping a cyberattack in its earlier stages, with typical indicators of compromise being IP addresses, file names, cryptographic file summaries, malicious domains and domains of management and control of cyber attackers
4. *public service media provider* is a media service provider as defined in Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) (Text with EEA relevance) (OJ L, 17.4.2024).
5. *competent authorities for the categorisation of entities* are competent authorities for the implementation of cybersecurity requirements, and competent authorities for the implementation of special laws, according to the division of competences set out in Annex III to the Act
6. *the competent authority for maintaining a special registry of entities* is the Security and Intelligence Agency
7. *entities required to submit data for the categorisation of entities* are the entities listed in Annexes I and II to the Act
8. *entities required to submit data for the maintenance of a special registry of entities* are DNS service providers, ccTLD name registries, registrars, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, of online search engines and of social networking services platforms
9. *operational technology (OT)* represents a wide range of programmable systems and devices that interact with the physical environment in a certain way or control other devices that interact with the physical environment and detect or cause a direct change in the physical environment through the monitoring and/or management of devices, processes and events
10. *persons responsible for managing cybersecurity risk-management measures* are members of the management bodies of essential and important entities, i.e. heads of state administration authorities, other state authorities and executive bodies of local and regional self-government units
11. *service recipient* is any natural and legal person to whom an essential or important entity provides a service based on the Act or a contract to provide services. A service contract

is a contract governing the provision and use of a service or other legally binding document that governs the legal relationship between a recipient of a service and an essential or important entity as a service provider, including the entity's general terms and conditions and other pre-drafted written rules by which the entity regulates legal relations with recipients of its services in advance

12. *applied scientific research* is industrial research, experimental development, or a combination thereof. Industrial research is planned research or a critical review aimed at acquiring new knowledge and skills to develop new products, processes, or services or to achieve significant improvements in existing ones. Experimental development involves the acquisition, combination, design, and application of existing scientific, technological, business, and other relevant knowledge and skills to create new or improved products, processes, or services. Experimental development may include activities to design, plan and document new products, processes or services
13. *reduced level of service quality* is a level of service quality that is lower than the prescribed or contracted level of service quality
14. *impact on authenticity* is the effect on the characteristic that an entity is what it claims to be
15. *impact on integrity* is the effect on the characteristic of accuracy and completeness
16. *impact on availability* is the effect on the continuity of service provision, a decrease in the level of service quality and partial or complete interruption of service provision
17. *impact on confidentiality* is the effect on the characteristic of availability in such a way that the information is available to unauthorised persons, individuals, entities or processes
18. *service* is any service explicitly listed in Annexes I and II to the Act, as well as any other service provided by an essential or important entity according to laws or other regulations within the scope of carrying out activities listed in Annex I and Annex II to the Act.

(2) Other terms used in this Regulation shall have the same meaning as the terms used in the Act.

(3) The terms used in this Regulation which are gender-specific, refer equally to the male and female gender.

Article 5

The provisions of this Regulation relating to the competent authorities for the implementation of cybersecurity requirements shall also apply to the competent authorities for the implementation of special laws when those provisions regulate issues related to cybersecurity requirements and their implementation, which are not regulated by special laws and by-laws adopted based on those laws, within the meaning of Article 8 of the Act.

Article 6

The competent authorities listed in Annex III to the Act and the single points of contact shall, under European Union law and relevant national law, safeguard the security and commercial interests of essential and important entities, as well as the confidentiality of the information provided, in the implementation of their obligations under this Regulation.

PART TWO

CATEGORISATION OF ENTITIES BASED ON SPECIAL CRITERIA, CATEGORISATION OF PUBLIC SECTOR AND EDUCATION SYSTEM ENTITIES

CHAPTER I
CRITERIA FOR THE CATEGORISATION OF ENTITIES BASED ON SPECIAL CRITERIA

Article 7

(1) Classification of entities under Article 11, subparagraph 1 of the Act is implemented for private and public entities listed in Annex I and Annex II to the Act, for which it is determined in the procedure of entity categorisation that in the area of at least one county, regardless of the number of inhabitants of its cities and municipalities, they are the sole provider of the service for which the entity is subject to categorisation of entities.

(2) Based on the criteria under paragraph 1 of this Article:

– private and public entities listed in Annex I to the Act shall be classified as essential entities

– private and public entities listed in Annex II to the Act shall be classified as important entities.

Article 8

(1) Classification of entities under Article 11, subparagraph 2 of the Act, according to the criterion of the significance of the impact that a disruption in the functioning of the service provided by the entity, i.e. the activity it performs, might have on public security, shall be carried out for private and public entities listed in Annex I and Annex II to the Act from which products are directly supplied or services are directly ordered, that are covered by Annex I or Annex II to the Act and that are used for:

– police purposes
– border surveillance, or
– protection and rescue in major accidents, disasters and crises.

(2) Based on the criteria under paragraph 1 of this Article:

– private and public entities listed in Annex I to the Act shall be classified as essential entities

– private and public entities listed in Annex II to the Act shall be classified as important entities.

(3) The categorisation of entities under paragraph 1 of this Article shall be conducted based on a reasoned request of the state administration authority in charge of internal affairs.

Article 9

(1) Classification of entities under Article 11, subparagraph 2 of the Act, according to the criterion of the significance of the impact that a disruption in the functioning of the service provided by the entity, i.e. the activity it performs, might have on public protection, shall be carried out for private and public entities listed in Annex I and Annex II to the Act that are:

– designated by the decisions of the competent state administration authority as operational forces of the civil protection system of special interest at the state level, or

– designated by the decisions of executive bodies of local and regional self-government units as a legal entity of interest for the civil protection system.

(2) Based on the criteria under paragraph 1, subparagraph 1 of this Article, private and public entities under Annex I and Annex II to the Act are classified as essential entities.

(3) Based on the criteria under paragraph 1, subparagraph 2 of this Article, private and public entities under Annex I and Annex II to the Act are classified as important entities.

(4) The categorisation of entities under paragraph 1 of this Article shall be conducted based on a reasoned request of the state administration authority in charge of the establishment of the civil protection system.

Article 10

(1) Classification of entities under Article 11, subparagraph 2 of the Act, according to the criterion of the significance of the impact that a disruption in the functioning of the service provided by the entity, i.e. the activity performed by the entity, might have on public health, shall be carried out for health care providers from Annex I to the Act who provide one of the following health care activities:

- combating infectious diseases
- supplying health care with medicinal products and medical devices
- collecting and preparing medicinal preparations and transplants of human origin, or
- emergency medicine.

(2) Based on the criteria under paragraph 1 of this Article, health care providers under Annex I to this Act shall be classified as essential entities, regardless of whether they provide health care activities under paragraph 1 of this Article at the primary, secondary or tertiary level.

(3) The categorisation of entities under paragraph 1 of this Article shall be conducted based on a reasoned request of the state administration authority in charge of health.

Article 11

(1) Classification of entities under Article 11, subparagraph 3 of the Act shall be carried out for private and public entities from the energy sector, the transport sector, the digital infrastructure sector, as well as managed service providers and managed security service providers from the ICT service management (B2B) sector under Annex I to the Act, for which it is determined in the procedure of categorisation of entities that the market share of the entity in the provision of services, i.e. the performance of the activity for which the entity is subject to the categorisation of entities, in the territory of the Republic of Croatia is 25% or more.

(2) Classification of entities under Article 11, subparagraph 3 of the Act shall also be carried out for managed service providers and managed security service providers from the ICT service management (B2B) sector under Annex I to the Act, which provide managed services and managed security services to essential and important entities.

(3) Private and public entities from the energy sector, the transport sector, the digital infrastructure sector and managed service providers and managed security service providers from the ICT service management (B2B) sector under Annex I to the Act shall be classified as essential entities based on the criteria under paragraph 1 of this Article.

(4) Managed service providers and managed security service providers from the ICT service management (B2B) sector under Annex I to the Act shall be classified as important entities based on the criteria under paragraph 2 of this Article.

Article 12

(1) Classification of entities under Article 11, subparagraph 4 of the Act, according to the criterion of special importance of the entity at the national level, shall be carried out for private and public entities listed in Annex I and Annex II to the Act, designated by the decision of the Government of the Republic of Croatia as a legal entity of special interest for the Republic of Croatia.

(2) Private and public entities under Annex I to the Act shall be classified as essential entities based on the criteria under paragraph 1 of this Article.

(3) Private and public entities listed in Annex II to the Act shall be classified as important entities based on the criteria under paragraph 1 of this Article.

(4) Classification of entities under Article 11, subparagraph 4 of the Act, according to the criterion of special importance of the entity at the regional and local level, is conducted for:

– private and public entities from the energy sector, the electricity subsector, the district heating and cooling subsector, the gas subsector, human consumption water sector and the wastewater sector under Annex I to the Act

– private and public entities from the postal and courier services sector under Annex II to the Act for which it is determined in the procedure of categorisation of entities that the market share of the entity in the provision of services, i.e. the performance of the activity for which the entity is subject to the categorisation of entities, in one county, regardless of the number of inhabitants of its cities and municipalities, is 40% or more.

(5) Private and public entities from the energy sector, the electricity subsector, the district heating and cooling subsector, the gas subsector, the human consumption water sector and the wastewater sector under Annex I to the Act shall be classified as essential entities based on the criteria under paragraph 4 of this Article.

(6) Private and public entities from the postal and courier services sector under Annex II to the Act shall be classified as important entities based on the criteria under paragraph 4 of this Article.

Article 13

The criteria for categorisation based on the special criteria set out in Articles 7 to 12 of this Regulation shall apply to the private and public entities listed in Annexes I and II to the Act, not classified based on the general criteria for the categorisation of entities under Articles 9 and 10 of the Act.

CHAPTER II
CATEGORISATION OF PUBLIC SECTOR AND EDUCATION SYSTEM ENTITIES

Article 14

(1) State authorities and legal persons with public authority shall be classified as essential entities if they meet the following criteria:

– the founder of the entity is the Republic of Croatia, it was established for the territory of the Republic of Croatia, it carries out its activities at the national level and is not categorised in any other sector of high criticality or other critical sector from Annex I and Annex II to the Act, and

– the impact of a significant cyber incident and a significant cyber threat on the network and information system of that entity may cause significant:

1. consequences for human life and health or the environment
2. material and non-material damage to that entity or other legal and natural persons
3. disruption in the entity's performance of regular activities
4. cross-sectoral consequences (impact on other sectors of social or economic activities) or
5. negative public impacts.

(2) When categorising public sector entities, the competent authority for the implementation of cybersecurity requirements shall evaluate the criteria under paragraph 1, subparagraph 2 of this Article, assessing each consequence of the impact of a significant cyber incident and a significant cyber threat separately and in relation to other consequences.

Article 15

Local and regional self-government units shall be classified as important entities if they meet at least one of the following criteria:

– they perform tasks of regional importance
– they represent the economic, financial, cultural, health, transport and scientific centres of development of the wider environment
– they are authorised to conduct activities in the field of economic development and planning, and the development of a network of educational, health, social and cultural institutions, or
– they were entrusted with state administration tasks.

Article 16

Entities from the education system are classified under Article 13 of the Act as important entities based on the assessment of their special importance for the performance of work relating to education and care if they meet at least one of the following criteria:

– they provide e-services of national information systems relevant to the education and care system in the Republic of Croatia

– they represent a higher education institution that conducts applied scientific research for the purpose of innovation and development of technologies, regardless of the founder of the institution

– they represent a higher education institution that provides services to information systems relevant for the education system in the Republic of Croatia, or

– they represent a public institution that conducts external evaluations of the education and care system of the Republic of Croatia and exams based on national standards.

PART THREE
LISTS OF ESSENTIAL AND IMPORTANT ENTITIES AND A SPECIAL REGISTRY OF ENTITIES

CHAPTER I
OBLIGATIONS OF ENTITIES UNDER ANNEX I AND ANNEX II TO THE ACT

Article 17

(1) Entities required to submit data for the categorisation of entities and entities required to submit data for the maintenance of a special registry of entities shall appoint a contact person responsible for the submission of data.

(2) The contact person responsible for the submission of data must be:

– a person appointed from among the members of the entity's management body

– a person appointed from among the state officials in state administration authorities and other state authorities, or

– an appointed executive body of the local and regional self-government unit.

Article 18

(1) The contact person responsible for the submission of data is responsible for the timely delivery of accurate and complete data and notifications of data changes under Articles 20 and 23 of the Act and the provisions of this Regulation.

(2) The contact person responsible for the submission of data shall appoint at least two persons authorised to operationalise the submission of data and notifications of changes to the data under Articles 20 and 23 of the Act.

Article 19

(1) Entities required to submit data for the categorisation of entities and entities required to submit data for the maintenance of a special registry of entities shall submit information on the appointed contact person responsible for the submission of data and persons authorised to operationalise the said submission to the competent authority for the categorisation of entities or the competent authority for the maintenance of the special registry of entities, without delay, and no later than eight days from the date of receipt of the request under Article 20, paragraph 1 and Article 23, paragraph 2 of the Act, as follows:

– name and surname of the appointed persons

– information concerning their job or duties in the entity

– email address of the contact person responsible for submitting the data, and

– email addresses to be used by persons authorised to operationalise submission for the purposes of submitting data and notifications of data changes.

(2) In the event of changes to the persons under paragraph 1 of this Article or data submitted under paragraph 1 of this Article, the entities required to submit data for the categorisation of entities and the entities required to submit data for the maintenance of a special registry of entities shall notify the competent authority for the categorisation of entities or the competent authority for maintaining a special registry of entities of the change, without delay, and no later than within 15 days from the date of appointment of a new person or change of the data submitted under paragraph 1 of this Article.

(3) The notifications under paragraphs 1 and 2 of this Article shall be submitted to the competent authority for the categorisation of entities or to the competent authority for maintaining a special registry of entities according to the instructions under Article 22 of this Regulation.

Article 20

Entities required to submit data for the categorisation of entities shall submit to the competent authority for the categorisation of entities the data and notifications of changes to the data under Article 20 of the Act as follows:

– '*name of the entity'*, meaning the name under which the entity operates or performs its activity in the Republic of Croatia, with an indication of the abbreviated name, if the entity uses it in legal transactions, and the personal identification number of the entity (hereinafter: PIN)

– '*address*', meaning the address of the entity's registered office and the address of the contact person responsible for the submission of data if it is different from the address of the entity's registered office

– '*up-to-date contact details, including email addresses'*, meaning the address of the entity's website, name and surname of the contact person responsible for the submission of data and persons authorised to operationalise the submission of data, telephone numbers, mobile phone numbers and email addresses of the contact person responsible for the submission of data and persons authorised to operationalise the submission of data

– '*IP address ranges'*, meaning the IP address ranges used by the entity in the Republic of Croatia

– '*relevant sector, subsector and type of entity referred to in Annex I and Annex II to the Act*', meaning the names of the sector, subsector and type of entity, as under Annex I to this Regulation

– '*list of Member States where the entity provides services falling within the scope of the Act'*, meaning a list of Member States of the European Union (hereinafter: Member States) where the entity provides services or carries out activities under Annex I or Annex II to the Act and the legal form of providing or performing these activities in other Member States, and

– *'other information on the provision of its services or the performance of its activities relevant for the categorisation of the entity or the determination of jurisdiction over the entity'*, meaning data on the size of the entity and other information requested from the entity by the competent authority to conduct the categorisation of the entity or determine jurisdiction over the entity.

Article 21

Entities required to submit data for the maintenance of the special registry of entities shall submit to the competent authority for the maintenance of the special registry of entities the data and notifications of changes to the data under Article 23 of the Act as follows:

– *'name of the entity'*, meaning the name under which the entity operates or performs its activity in the Republic of Croatia, with an indication of the abbreviated name, if the entity uses it in legal transactions, and PIN

– *'address of the entity's main establishment*', meaning the address of the main establishment of the entity within the meaning of Article 14, paragraphs 3 and 4 of the Act

– *'list of services under Article 22 of the Act'*, meaning the list of services under Article 22 of the Act provided by the entity in the Republic of Croatia

– *'addresses of establishments in the Republic of Croatia'*, meaning the addresses of all establishments of the entity located in the Republic of Croatia

– *'IP address ranges'*, meaning the IP address ranges used by the entity in the Republic of Croatia

– *'list of other Member States where the entity operates'*, meaning a list of other Member States where the entity provides the services under Article 22 of the Act

– *'addresses of other establishments'*, meaning the addresses of the establishments of the entity where the entity provides the services under Article 22 of the Act that exist in other Member States, and

– '*up-to-date contact details, including email addresses and telephone numbers of the entity'*, meaning the address of the entity's website, name and surname of the contact person responsible for the submission of data, telephone number, mobile phone number and email address of the contact person responsible for the submission of data, if the entity has its main establishment in the Republic of Croatia within the meaning of Article 14, paragraphs 3 and 4 of the Act, or

– *'name and address of the representative, up-to-date contact details, including email addresses and telephone numbers of the representative'*, meaning the name, address, telephone number, mobile phone number and email address of a natural or legal person established in the Republic of Croatia or another Member State, who has been expressly appointed to act on behalf of the entity required to submit data for the maintenance of a special registry of entities not established in the European Union and to whom the competent authority may address in place of the entity itself with regard to the obligations of that entity under this Regulation.

Article 22

(1) The data under Articles 20 and 21 of this Regulation and the notifications of their change shall be submitted in electronic form, following the instructions published on their websites by the competent authorities for the categorisation of entities and the competent authority for maintaining a special registry of entities.

(2) The competent authorities for the categorisation of entities and the competent authority for maintaining a special registry of entities shall define in the instructions under paragraph 1 of this Article, the manner of submission in exceptional cases when submission in electronic form is not possible for justified reasons.

(3) The competent authority for maintaining the special registry of entities shall define, in the instructions under paragraph 1 of this Article, the manner of compiling and submitting data and notifications of data changes if the same entities are required to submit data and notifications on data changes based on obligations arising for these entities as the entity required to submit data for maintaining a special registry of entities and the entity required to submit data for the categorisation of entities.

Article 23

(1) The instructions under Article 22 of this Regulation shall also contain instructions for the voluntary submission of data to conduct the process of categorisation of the entity.

(2) The submission of data on the entity following the instructions for voluntary submission of data under paragraph 1 of this Article shall be considered equivalent to the submission of data at the request of the competent authority for the implementation of cybersecurity requirements under Article 20, paragraph 1 of the Act.

(3) The submission of data on the entity under paragraphs 1 and 2 of this Article shall not affect the obligation to notify the entity of the categorisation carried out under Article 19 of the Act.

(4) The submission of data on the entity under paragraphs 1 and 2 of this Article shall not affect the obligations of the entity under Articles 17 to 19 of this Regulation.

Article 24

(1) If the data or notifications of data changes have not been submitted in accordance with Articles 19 to 23 of this Regulation, the competent authority for the categorisation of entities and the competent authority for maintaining a special registry of entities shall notify the entity thereof and set a deadline within which the entity must remedy the deficiencies and submit the data or the amendment, supplement or correction of the data, with a warning of legal consequences under the Act if the entity fails to do so within the given deadline.

(2) The notification under paragraph 1 of this Article shall be submitted to the email address of the contact person responsible for the submission of data or the email address of the representative of the entity required to submit the data for maintaining a special registry of entities not established in the European Union.

CHAPTER II
COLLECTING DATA FROM OTHER SOURCES

Article 25

(1) To implement the obligations under Article 21, subparagraph 1 of the Act, state administration authorities, other state authorities, local and regional self-government units, legal persons with public authority and public entities are required to keep a list of entities from Annex I and Annex II to the Act, for which they collect data within their scope of competence, i.e. maintain registries, records and data collections.

(2) The list of entities under paragraph 1 of this Article shall contain the following information:

- sectors, subsectors and types of entities listed in Annexes I and II to the Act, for which they collect data, i.e. maintain registries, records and data collections, according to the names listed in Annex I to this Regulation
- for each sector, subsector and type of entity under subparagraph 1 of this paragraph, the names of the entities or the names under which the entities operate or conduct the activities under Annex I and Annex II to the Act in the Republic of Croatia, with an indication of the abbreviated name, if the entity uses it in legal transactions
- the legal basis on which they collect data, i.e. maintain registries, records and data collections on the entities under subparagraph 2 of this paragraph
- an indication of whether they maintain registries, records, and data collections relating to the size of entities within the meaning of Article 15 of the Act, and what data they collect, and
- information on whether they maintain registries, records and data collections for the entities under subparagraph 2 of this paragraph in electronic form, together with a statement on the possibilities of accessing the data in those registries, records and data collections electronically.

(3) The lists of entities under paragraph 1 of this Article shall be submitted following the instructions published by the competent authorities for the categorisation of entities on their websites.

(4) The lists of entities under paragraph 1 of this Article shall be submitted to the competent authorities for the categorisation of entities once a year, no later than by 1 March of the current year for the previous year.

(5) Notwithstanding paragraph 4 of this Article, if there have been no changes concerning the previously submitted list of entities, state administration authorities, other state authorities, local and regional self-government units, legal persons with public authority and public entities shall inform the competent authority for the categorisation of entities thereof, without the obligation to submit a new list of entities.

(6) Notwithstanding paragraphs 1 and 4 of this Article, state administration authorities, other state authorities, local and regional self-government units, legal persons with public authority and public entities shall not be required to maintain and regularly submit lists of entities under paragraph 1 of this Article, if they have provided the competent authorities for the categorisation of entities with electronic access to the relevant data on entities in the registries, records and data collections.

Article 26

Article 25 of this Regulation shall not apply to:

- the banking sector
- the financial market infrastructures sector and
- the air transport subsector.

CHAPTER III
METHOD OF MAINTAINING AND CONTENT OF THE LIST OF ESSENTIAL AND IMPORTANT ENTITIES

Article 27

(1) Lists of essential and important entities shall be maintained in electronic form.

(2) Lists of essential and important entities shall include the data prescribed by this Regulation and any changes to these data in such a way that they show the originally entered data and the subsequently entered changes to these data.

Article 28

(1) Lists of essential and important entities shall be maintained by sectors, subsectors and types of entities listed in Annexes I and II to the Act, according to the names from Annex I to this Regulation.

(2) Lists of essential and important entities shall contain general information about the entity and data on the conducted categorisation of the entity.

(3) The following information shall be entered in the lists of essential and important entities under '*general information about the entity'*:

- name of the entity
- PIN of the entity
- address of the entity
- telephone number, mobile phone number and email address of the contact person responsible for the submission of data
- IP address ranges used by the entity in the Republic of Croatia
- list of Member States where the entity provides services and carries out activities under Annex I and Annex II to the Act, respectively.
- date of entry of the entity in the list of essential and important entities.

(4) The following information shall be entered in the lists of essential and important entities under '*data on the conducted categorisation of the entity'*:

- information on the entity category, i.e. an indication of whether the entity is classified as an essential and/or important entity
- information about the provision of the Act based on which the entity categorisation was carried out
- name of the sector, subsector and type of entity to which the entity is classified, according to the names set out in Annex I to this Regulation
- date of the entity's categorisation
- level of cybersecurity risk-management measures binding on the entity set out in Article 38 of this Regulation

- date of notification of the categorisation of the entity under Article 19, paragraphs 1 and 2 of the Act, when applicable
- note as to whether a protocol on the procedure of competent authorities under Article 59, paragraph 3 of the Act has been drawn up for the entity, when applicable
- date of verification of the list under Article 17, paragraph 2 of the Act.

(5) General information about the entity shall be entered in the list of essential and important entities based on the data submitted under Articles 19, 20, 22 and 23 of this Regulation.

(6) The data on the categorisation of the entity carried out and the binding level of cybersecurity risk-management measures shall be entered based on the data determined in the process of categorisation of the entity or the checks carried out on the list of essential and important entities under Article 17, paragraph 2 of the Act.

Article 29

(1) The competent authorities for the categorisation of entities shall enter the entity in the list of essential and important entities no later than eight days from the date of the categorisation of the entity.

(2) The competent authorities for the categorisation of entities shall enter the change of the entity's category and other related data in the list of essential and important entities no later than eight days from the date of delivery of the notification under Article 19, paragraph 2 of the Act.

(3) The competent authorities for the categorisation of entities shall enter changes to the general data about the entity within eight days from the date of receipt of the notification of changes to the data under Articles 19 and 20 of this Regulation.

Article 30

(1) The competent authorities for the categorisation of entities shall list entities that are, after the update of the list of essential and important entities, no longer considered to be either essential entities or important entities in the list of essential and important entities with the indication 'inactive'.

(2) The competent authorities for the categorisation of entities shall also include in their verifications of the list of essential and important entities under Article 17, paragraph 2 of the Act, the entities under paragraph 1 of this Article unless it has been established that the entity has ceased operations in the preliminary verification procedure.

Article 31

(1) To implement the obligations under Article 18, paragraph 2 of the Act, the competent authorities for the categorisation of entities shall submit the data on the conducted categorisation of entities to the single point of contact following the guidelines of the single point of contact on the content, method of submission and deadlines for the submission of notifications of the conducted categorisation of entities.

(2) To implement Article 43 of the Act, the competent authorities for the categorisation of entities shall submit the lists of essential and important entities, including all subsequent updates of the lists, in due time and in the appropriate format to the Croatian Academic and Research Network – CARNET (hereinafter: CARNET).

CHAPTER IV
METHOD OF MAINTAINING AND CONTENT OF THE SPECIAL REGISTRY OF ENTITIES

Article 32

(1) The special registry of entities shall be maintained in electronic form.

(2) The data prescribed by this Regulation and any changes to these data shall be entered in the special registry of entities in such a way that they show the originally entered data and the subsequently entered changes to these data.

Article 33

(1) The special registry of entities shall contain the following information:

- name of the entity
- PIN of the entity
- list of services under Article 22 of the Act provided by the entity in the Republic of Croatia
- address of the entity's main establishment
- addresses of the establishments of the entity in the Republic of Croatia
- IP address ranges used by the entity in the Republic of Croatia
- list of other Member States where the entity provides the services under Article 22 of the Act
- addresses of the establishments of the entity where the entity provides the services under Article 22 of the Act that exist in other Member States
- telephone number, mobile phone number and email address of the contact person responsible for the submission of data or a representative of the entity if the entity is not established in the European Union
- date of entry of the entity in the special registry of entities.

(2) The data on the entity shall be entered in the special registry of entities based on the data submitted under Articles 19, 21 and 22 of this Regulation.

Article 34

To implement the obligations under Article 23, paragraph 4 of the Act, the competent authority for maintaining a special registry of entities shall submit information on the entities under Article 22 of the Act through the single point of contact, to the European Union Agency for Cybersecurity (hereinafter: ENISA) within the deadlines and in the manner defined in its guidelines.

PART FOUR
MANAGING CYBERSECURITY RISKS

CHAPTER I
NATIONAL CYBERSECURITY RISK ASSESSMENT

Article 35

(1) As part of the entity categorisation process, a national cybersecurity risk assessment (hereinafter: national risk assessment) is conducted for each entity categorised as an essential or important entity.

(2) The aim of conducting a national risk assessment is to define the level of cybersecurity risk-management measures to be implemented by each entity that is categorised as essential or important.

Article 36

The national risk assessment is carried out based on data about:

- the size of the entity, and
- whether it belongs to a particular sector listed in Annexes I and II to the Act, as well as based on monitoring the state of cybersecurity at the global and national level and conducting related assessments:
- selection of typical types of cyberattacks, which are considered relevant for this assessment, such as business disruption or sabotage, data theft or espionage, cybercrime, vandalism of content and availability of data on the internet, political influence and disinformation
- whether a particular type of typical cyberattacks is generally possible in a particular sector or is it assessed as targeted for a particular sector
- level of severity of disruptions in the functioning of services or the carrying out of activities that selected types of typical cyberattacks can cause in a particular sector, according to available data
- selection of typical types of cyber attackers to be considered relevant for this assessment, such as state-sponsored APT groups, terrorists, cybercriminal groups, hacktivist groups, and competing business attackers, together with an assessment of the typical level of cyber skills of the selected types of attackers
- occurrence probability of each type of cyberattack, caused by a particular type of cyber attacker for each sector, for all selected typical types of cyberattacks, as well as for all selected types of cyber attackers.

Article 37

(1) The necessary elaboration of the data and assessments under Article 36 to conduct a national risk assessment for entities in the sectors listed in Annex I and Annex II to the Act shall be implemented by the central government authority for cybersecurity, in cooperation with other competent authorities for the implementation of cybersecurity requirements.

(2) Based on the data and assessments under paragraph 1 of this Article, the national risk assessment for each entity, which is categorised in the area of competence of each competent authority for the implementation of cybersecurity requirements, shall be carried out by the competent authority for the implementation of cybersecurity requirements.

(3) The national risk assessment under paragraph 2 of this Article shall be carried out as part of the first procedure for the categorisation of an entity, following each update of the list of essential and important entities under Article 17, paragraph 2 of the Act and during each categorisation of an entity carried out by the competent authority for the implementation of cybersecurity requirements.

Article 38

(1) The result of the national risk assessment shall be the identification of a low, medium or high level of cybersecurity risks for each entity under Article 37, paragraph 2 of this Regulation.

(2) Depending on the level of cybersecurity risks identified, each entity that is categorised as an essential or important entity shall be required to implement one of three levels of cybersecurity risk-management measures, as follows:

- for a low level of assessed cybersecurity risks, the categorisation shall require the entity to implement a basic level of cybersecurity risk-management measures under Article 42, paragraph 1 and Annex II to this Regulation
- for a medium level of assessed cybersecurity risks, the categorisation shall require the entity to implement an intermediate level of cybersecurity risk-management measures under Article 42, paragraph 2 and Annex II to this Regulation
- for a high level of assessed cybersecurity risks, the categorisation shall require the entity to implement an advanced level of cybersecurity risk-management measures under Article 42, paragraph 3 and Annex II to this Regulation.

Article 39

(1) Where an entity provides services or carries out activities belonging to several different sectors listed in Annexes I and II to the Act, the national risk assessment is carried out for the main activity of the entity.

(2) If the main activity of the entity cannot be unequivocally determined, the national risk assessment shall be carried out for all services and activities for the provision or carrying out of which the entity is categorised as an essential or important entity, and the highest level of cybersecurity risks thus determined shall be taken as the final national risk assessment of the entity.

Article 40

(1) The national risk assessment and the determination of a level of cybersecurity risk-management measures binding on essential and important entities under Article 38 of this Regulation shall be carried out following the guidelines for the implementation of the national cybersecurity risk assessment, which shall be prepared based on the data and assessments under Article 36 of this Regulation and which shall include the corresponding calculator for calculating the level of cybersecurity risks.

(2) The guidelines for the implementation of the national risk assessment under paragraph 1 of this Article, describing the risk calculation procedure based on the data and assessments under Article 36 of this Regulation, as well as the use of the corresponding calculator, shall be adopted by the central government authority for cybersecurity.

(3) The central government authority for cybersecurity shall publish the guidelines under paragraph 2 of this Article on its website.

CHAPTER II
CYBERSECURITY RISK-MANAGEMENT MEASURES

Article 41

The list of cybersecurity risk-management measures is set out in Annex II to this Regulation for all three levels of cybersecurity risk-management measures under Article 38 of this Regulation.

Article 42

(1) The basic level of cybersecurity risk-management measures under Article 38, paragraph 2, subparagraph 1 of this Regulation shall constitute a general set of cybersecurity practice measures that can be achieved with readily available technologies and well-known and documented cybersecurity best practices, appropriate for entities whose activities belong to sectors that are not typical of targeted cyberattacks carried out by attackers with a higher level of cyber skills, and the aim of applying the basic level is to protect the entity from the majority of globally present cyberattacks, i.e. from cyberattacks carried out by cyber attackers of average cyber skills.

(2) The intermediate level of cybersecurity risk-management measures under Article 38, paragraph 2, subparagraph 2 of this Regulation shall constitute a supplemented set of cybersecurity practice measures that builds on the basic level of cybersecurity risk-management measures, and the aim of applying the intermediate level is to further reduce the risks of targeted cyberattacks carried out by cyber attackers of average cyber skills.

(3) The advanced level of cybersecurity risk-management measures under Article 38, paragraph 2, subparagraph 3 of this Regulation shall constitute a supplemented set of cybersecurity practice measures that builds on the intermediate level of cybersecurity risk-management measures, and the aim of applying the advanced level is to reduce the risks of advanced cyberattacks carried out by cyber attackers with advanced skills and resources.

Article 43

The list of cybersecurity risk-management measures set out in Annex II to this Regulation shall include, for each measure:

- the name of the measure
- the objective of the measure
- the elaboration of the measure into subsets of cybersecurity risk-management measures
- the applicability of the measure in the context of IT and OT systems, and
- the tabular presentation of the distribution of subsets of measures under subparagraph 3 of this paragraph by the levels of measures under Article 38 of this Regulation.

Article 44

(1) Subsets of cybersecurity risk-management measures, the implementation of which within a certain level of measures under Article 38 of this Regulation is binding, shall be marked with ‘A’ in the table under Article 43, subparagraph 5 of this Regulation.

(2) Subsets of cybersecurity risk-management measures, the implementation of which within a certain level of measures under Article 38 of this Regulation is binding under the conditions described in the elaboration of the measure under Article 43, subparagraph 4 of this Regulation under ‘CONDITION:’, shall be marked with ‘B’ in the table under Article 43, subparagraph 5 of this Regulation.

(3) Subsets of cybersecurity risk-management measures, the implementation of which within a certain level of measures under Article 38 of this Regulation is voluntary, shall be marked with ‘C’ in the table under Article 43, subparagraph 5 of this Regulation.

Article 45

(1) Subsets of cybersecurity risk-management measures that are marked with ‘C’ in the table under Article 43, subparagraph 5 of this Regulation, shall be recommended to be implemented depending on the results of the risk assessment carried out by the entity as part of the implementation of the measure called ‘Risk management’ under point 3 of Annex II to this Regulation.

(2) The implementation of subsets of cybersecurity risk-management measures marked with ‘C’ in the table under Article 43, subparagraph 5 of this Regulation shall be further evaluated through the process of cybersecurity self-assessment and cybersecurity audit.

(3) To conduct the risk assessment under paragraph 1 of this Article, the central government authority for cybersecurity shall adopt guidelines for the assessment, processing, monitoring and updating of risks for network and information systems, which may be used within the implementation of the measure entitled ‘Risk management’ under point 3 of Annex II to this Regulation.

(4) The central government authority for cybersecurity shall publish the guidelines under paragraph 3 of this Article on its website.

Article 46

(1) The services provided, or the activities carried out by private and public entities in the digital infrastructure sector listed in Annex I to the Act are based on network and information systems, and this Regulation establishes a specific, extended set of physical security measures for these types of entities as part of the cybersecurity risk-management measures that these entities are required to implement.

(2) The extended set of physical security measures under paragraph 1 of this Article is set out in Annex III to this Regulation.

Article 47

(1) With the purpose of implementing the voluntary cyber protection mechanisms under Article 50 of the Act, entities that are not categorised as essential and important entities implement at least a basic level of cybersecurity risk-management measures.

(2) In the cases under Article 60 of the Act, the competent authorities for the implementation of cybersecurity requirements are required to implement an advanced level of cybersecurity risk-management measures.

Article 48

Any cybersecurity risk-management measures implemented, essential and important entities and entities under Article 47 of this Regulation must update:

- in planned periods and at least annually as part of the entity's regular annual risk assessment
- in the event of a significant incident
- in case of significant changes to the network and information system
- as part of major business and organisational changes, mergers or changes in the ownership structure of the entity that may have an impact on the management of the entity
- when an entity is found to be non-compliant in the cybersecurity audit or cybersecurity self-assessment process, or
- when corrective actions are imposed on the entity during expert supervision of the implementation of cybersecurity requirements.

Article 49

(1) To facilitate the implementation of cybersecurity risk-management measures, the central government authority for cybersecurity shall prepare a correlation overview of the measures under Annex II to this Regulation, as well as of all subsets of these measures, to the most important European and international standards and best practices from open sources (mapping of measures).

(2) The central government authority for cybersecurity shall publish the correlation overview under paragraph 1 of this Article on its website.

Article 50

To raise the level of cybersecurity of entities that are not categorised as essential or important entities and do not implement voluntary cyber protection mechanisms under Article 50 of the Act, entities that are just starting to introduce cybersecurity risk-management measures or entities that represent a micro or small business entity with limited resources and knowledge in cybersecurity risk-management issues, the central government authority for cybersecurity shall prepare and publish on its website recommendations for the implementation of good cybersecurity practices.

CHAPTER III
CYBERSECURITY SELF-ASSESSMENT

Article 51

(1) The cybersecurity self-assessment shall determine the degree of compliance of the established cybersecurity risk-management measures with the cybersecurity risk-management measures set out in Annex II to this Regulation established for the level of cybersecurity risk-management measures under Article 38 of this Regulation that the entity is required to implement, as well as the trend of raising the level of cybersecurity maturity of the entity.

(2) Important entities and entities under Article 47 of this Regulation shall carry out a cybersecurity self-assessment at least once every two years.

(3) Essential entities may conduct a cybersecurity self-assessment in preparation for conducting a cybersecurity audit or expert supervision of the implementation of cybersecurity requirements under Article 75, paragraph 1 of the Act.

Article 52

(1) The degree of compliance of the established measures shall be based on assessing the degree of compliance of the entity's documented and implemented cybersecurity risk-management measures.

(2) The assessment of the degree of compliance of the documented cybersecurity risk-management measures shall determine whether documented security policies on the implementation of the measures exist and to what extent they comply with the requirements set out for cybersecurity risk-management measures in Annex II to this Regulation, for the level of cybersecurity risk-management measures under Article 38 of this Regulation that the entity is required to implement.

(3) The assessment of the degree of compliance of the implemented cybersecurity risk-management measures shall determine the extent to which the cybersecurity risk-management measures in place comply with the requirements set out for cybersecurity risk-management measures in Annex II to this Regulation, for the level of cybersecurity risk-management measures under Article 38 of this Regulation that the entity is required to implement.

Article 53

(1) The degree of compliance of the established measures under Article 52, paragraphs 2 and 3 of this Regulation shall be determined based on scoring the subsets of cybersecurity risk-management measures implemented by the entity as binding under Article 44, paragraphs 1 and 2 of this Regulation.

(2) To perform the scoring under the previous paragraph of this Article, for each level of cybersecurity risk-management measures under Article 42 of this Regulation, the number of points necessary to confirm the entity's compliance with the level of cybersecurity risk-management measures determined as binding on the entity under Article 38 of this Regulation shall be determined.

Article 54

(1) The trend of raising the level of cybersecurity maturity shall be determined by additional scoring of subsets of cybersecurity risk-management measures implemented by the entity under Measure 3 'Risk management' under Annex II to this Regulation, in terms of raising the level of implementation of certain binding measures in accordance with Article 44, paragraphs 1 and 2 of this Regulation, as well as in terms of implementing voluntary measures in accordance with Article 44, paragraph 3 of this Regulation.

(2) To perform the scoring under the previous paragraph, for each level of cybersecurity risk-management measures under Article 42 of this Regulation, the number of points necessary to determine the trend of raising the level of cybersecurity maturity of the entity shall be determined.

Article 55

(1) If the results of the scoring of the degree of compliance of measures under Article 53 of this Regulation show that cybersecurity risk-management measures have been established in compliance with the level of cybersecurity risk-management measures determined as binding on the entity under Article 38 of this Regulation, the entity shall draw up a statement of compliance referred to in paragraph 3 of this Article.

(2) If the results of the scoring of the degree of compliance of measures under Article 53 of this Regulation show that cybersecurity risk-management measures have not been established in compliance with the level of cybersecurity risk-management measures determined as binding on the entity under Article 38 of this Regulation, the entity shall establish a follow-up plan, which shall include a plan for the timely cybersecurity self-reassessment and remedying of the identified deficiencies.

(3) The statement of compliance under Article 35, paragraph 3 of the Act contains the following information:

- the name and address of the entity
- the name of the sector, subsector and type of entity, according to the names set out in Annex I to this Regulation, for essential and important entities or
- the name of the sector and the main business activity for the entities under Article 47, paragraph 1 of this Regulation
- the level of cybersecurity risks identified for the entity, where applicable
- the level of cybersecurity risk-management measures determined as binding on the entity under Article 38 of this Regulation
- the results of scoring the degree of compliance of cybersecurity risk-management measures with the level of cybersecurity risk-management measures determined as binding on the entity under Article 38 of this Regulation
- the scoring results of the trend of raising the level of cybersecurity maturity of the entity
- the list of documentation created in the cybersecurity self-assessment process
- the name, surname and signature of the person who conducted the cybersecurity self-assessment procedure
- the statement by the person responsible for the management of cybersecurity risk-management measures that the results of the cybersecurity self-assessment

carried out for the entity show that cybersecurity risk-management measures have been established in compliance with the cybersecurity risk-management measures prescribed by the Act and this Regulation

- the name, surname and signature of the person responsible for managing cybersecurity risk-management measures.

(4) The entity shall draw up the statement of compliance under Article 35, paragraph 3 of the Act using the form from Annex IV to this Regulation.

(5) The entity shall keep the statement of compliance under Article 35, paragraph 3 of the Act, and other documentation created in the process of the cybersecurity self-assessment, for ten years from the date of drawing up of such a statement.

Article 56

To perform a cybersecurity self-assessment, the entity shall designate its employees or external associates who possess at least the following:

- relevant knowledge about the implementation of international standards in the field of information security or cybersecurity
- certificate of completion of external or internal training for an internal auditor according to one of the relevant international standards in the field of information security or cybersecurity
- one year of work experience in conducting similar types of internal audits in the field of network and information systems or cybersecurity.

Article 57

(1) The central government authority for performing tasks in the technical areas of information security shall adopt guidelines for the implementation of cybersecurity self-assessments, an integral part of which is a calculator for scoring and calculating the degree of compliance of established cybersecurity risk-management measures and the trend of raising the level of cybersecurity maturity of the entity.

(2) The central government authority for performing tasks in the technical areas of information security shall publish the guidelines under paragraph 1 of this Article on its website.

PART FIVE
RULES FOR THE NOTIFICATION OF CYBER THREATS AND INCIDENTS FOR ESSENTIAL AND IMPORTANT ENTITIES

CHAPTER I
NOTIFICATION OF SIGNIFICANT INCIDENTS

Article 58

A significant incident is any incident that meets at least one of the criteria for determining significant incidents set out in Articles 59 to 62 of this Regulation, considering the criteria thresholds, where prescribed.

SECTION 1
CRITERIA FOR DETERMINING SIGNIFICANT INCIDENTS

Article 59

(1) Incidents that cause or are capable of causing severe operational disruption of the services are incidents:

- that adversely affect the availability of the service or impair the quality of the service, or
- that adversely affect or are capable of adversely affecting the authenticity, integrity or confidentiality of stored, transmitted or processed data or services.

(2) An incident shall be considered to adversely affect the availability of the service or impair the quality of service if at least one of the following criteria thresholds is met:

- at least 20% of the recipients of the service were unable to access the service for at least one hour
- at least 1% of the recipients of the service were unable to access the service for at least eight hours, provided that 1% of the recipients are at least 100 recipients of the service
- access to the service was not possible for an hour or more, and the entity is not capable of determining how many recipients of the service were unable to access the service during the period in which the service was unavailable
- at least 30% of the recipients of the service were occasionally unable to access the service or were unable to use the service functionally due to a reduced level of service quality if the occasional interruptions to access the service, or the inability to use the service functionally, lasted for a total of at least one hour over a period of four hours
- access to the service in a hospital, airport, airline, bank facility with data centres, police system facility, active water pumping station and control centre, facility of an electronic communications operator, facility of a security and intelligence system body, facility of a professional fire brigade or entity that has been identified as critical entities based on the law governing the field of critical infrastructure, was not possible for at least one hour
- access to the air traffic control service was not possible, irrespective of the duration of the interruption of access to the service and the number of recipients to whom the service was unavailable
- access to the service used for the needs of the Ministry of Defence and the Armed Forces of the Republic of Croatia, civilian defence planning authorities, or for the needs of legal entities particularly important for defence, was not possible for at least one hour
- access to the service of the 112 Centre and other emergency services was not possible, regardless of the duration of the interruption of access to the service and the number of recipients to whom the service was unavailable

- access to the service in at least one county or one city or town representing the seat of the county was not possible for at least one hour.

(3) An incident shall be considered to adversely affect or be capable of adversely affecting the authenticity, integrity or confidentiality of stored, transmitted or processed data or services if at least one of the following criteria thresholds is met:

- critical parts of the entity's network and information system or critical data have been accessed by an unauthorised person, or the prerequisites have been met for an unauthorised person to gain access
- an unauthorised person has configured the entity's critical network and information systems, or the prerequisites have been met that enable the configuration of a critical network and information system by an unauthorised person
- due to the incident, circumstances have arisen that prevent an authorised person from configuring the critical network and information system
- the configuration of the entity's critical network and information system has been modified, supplemented, or otherwise rendered untrustworthy without authorisation, or critical data have been removed, altered, supplemented or otherwise rendered untrustworthy without authorisation
- the entity's critical network and information systems and/or other network and information systems of the entity that may affect the entity's critical network and information systems perform tasks that deviate from the established procedures for carrying out business activities on the system and/or the established control framework in which those systems normally operate, and in particular if they perform tasks that those systems are not intended to perform or do not perform the essential tasks that they are intended to perform.

(4) Within the meaning of paragraph 3 of this Article, all systems and data shall be considered as critical if the entity has not carried out the classification of the criticality of network and information systems, has not identified critical data or is unable to identify critical network and information systems or critical data that have been adversely affected by the incident.

Article 60

(1) An incident shall be considered to cause or be capable of causing financial loss to an entity if at least one of the following criteria thresholds is met:

- if the loss of revenue or costs caused by the incident, or the sum of the two, amounts to one hundred thousand euro or at least 5% of the entity's total annual operating revenue, whichever is lower
- if access to the service was not possible for at least one hour to recipients of services from whom the entity generated revenue of one hundred thousand euro in the previous year or at least 5% of the entity's total annual operating revenue, whichever is lower
- if the incident caused reputational damage to the entity.

(2) The total annual operating revenue of an entity within the meaning of paragraph 1 of this Article shall mean the total annual operating revenue of the entity according to the financial statements for the previous year, regardless of whether the entity also provides other services or carries out other activities not covered by Annex I and Annex II to the Act.

(3) The revenue within the meaning of paragraph 1 of this Article shall be deemed to be any revenue of an entity on an annual basis, regardless of whether it is generated

or planned to be generated through the entity's regular operations or through activities that go beyond the scope of the entity's regular operations.

(4) The costs within the meaning of paragraph 1 of this Article shall be deemed to be any costs incurred by the entity as a result of taking actions and activities to contain, respond to or recover from an incident, including all actions and activities undertaken to establish the entity's normal scope of operations. This shall not include contractual penalties or other types of compensation that the entity is required to pay due to a breach of contractual relations caused by the incident, regardless of whether the person involved is a natural or legal person, or employees or external associates of the entity.

(5) An incident shall be deemed to have caused reputational damage to an entity within the meaning of paragraph 1, subparagraph 3 of this Article if one of the following criteria thresholds is met:

- a public service media provider reported the incident
- the incident resulted in at least 1% of the recipients of the entity's services raising objections, filing lawsuits, or seeking other remedies against the entity.

Article 61

(1) An incident shall be considered to have affected or be capable of affecting other natural and legal persons by causing significant material or non-material damage if the incident resulted in one of the following:

- death or bodily injury that required hospitalisation or therapy procedures
- complete destruction or substantial damage to the material property of other natural or legal persons
- suspension or significant reduction of operations of other natural or legal persons
- loss or compromise of personal or sensitive data of other natural or legal persons.

(2) Other natural and legal persons within the meaning of paragraph 1 of this Article shall be considered recipients of services of an essential and important entity, as well as any other natural and legal person who has suffered material or non-material damage under paragraph 1 of this Article due to a significant incident.

Article 62

Incidents which individually do not meet the criteria for a significant incident set out in Articles 59 to 61 of this Regulation shall be considered as a significant incident if:

– they occurred at least twice in a six-month period
– they have the same root cause
– together they meet at least one of the criteria for a significant incident set out in Articles 59 to 61 of this Regulation.

Article 63

Interruptions in the provision of service or impairment of the quality of service due to planned routine maintenance of the network and information systems of essential and

important entities shall not be considered to be a significant incident within the meaning of Articles 59 to 62 of this Regulation.

SECTION 2
NOTIFICATIONS OF SIGNIFICANT INCIDENTS

Article 64

Essential and important entities shall notify the competent CSIRT of any significant incident.

Article 65

Essential and important entities shall submit the following types of significant incident notifications to the competent CSIRTs:

- early warning of a significant incident
- initial notification of a significant incident
- intermediate report on a significant incident
- progress report
- final report on a significant incident.

Article 66

(1) Essential and important entities shall submit an early warning of a significant incident to the competent CSIRT without delay and no later than within 24 hours from the moment of becoming aware of the significant incident.

(2) The early warning of a significant incident must include:

- date and time of becoming aware of the incident
- description of the basic characteristics of the incident
- information on whether the incident is suspected to have been caused by illegal or malicious activity
- entity’s assessment of whether the incident may have a cross-border impact
- entity’s assessment of whether the incident may have a cross-sectoral impact.

Article 67

(1) Essential and important entities shall submit the initial notification of a significant incident to the competent CSIRT without delay and no later than within 72 hours from the moment of becoming aware of the significant incident.

(2) The initial notification of a significant incident must include:

- updated description of the basic characteristics of the incident and other information submitted under Article 66 of this Regulation
- initial assessment of the significant incident
- indicators of compromise, if available.

(3) The initial assessment of a significant incident shall include an assessment by the essential and important entity of:

- the network and information system of the entity that was affected by the incident, and the importance of that system for the provision of services or carrying out of the activities of the entity
- the severity and impact of the incident, considering the extent to which the provision of services or the carrying out of the activities of the entity is threatened, the duration of the incident and the number of recipients of services affected by the incident
- technical characteristics of the incident
- vulnerabilities that are being exploited
- the entity's experience with similar incidents.

Article 68

By way of derogation from Article 66, paragraph 1 of this Regulation and Article 67, paragraph 1 of this Regulation, trust service providers shall submit to the competent CSIRT without delay and no later than within 24 hours from the moment of becoming aware of a significant incident, an initial notification of the significant incident, including information on the date and time of becoming aware of the incident.

Article 69

(1) Essential and important entities shall submit an intermediate report on a significant incident at the request of the competent CSIRT.

(2) In the request under paragraph 1 of this Article, the competent CSIRT shall determine:

- the data under Article 67 of this Regulation to which the request relates
- the deadline for the submission of the intermediate report on a significant incident.

(3) The deadline for the submission of the intermediate report on a significant incident shall be determined depending on the scope and complexity of the data to which the request under paragraph 1 of this Article relates, provided that the deadline may not be shorter than 48 hours or longer than seven days from the receipt of the request for the submission of the intermediate report.

(4) If it deems it necessary, the competent CSIRT may submit the requests under paragraph 1 of this Article repeatedly until the submission of the final report on a significant incident.

Article 70

(1) The final report on a significant incident shall be submitted by essential and important entities to the competent CSIRT no later than within 30 days from the date of submitting the initial notification of a significant incident.

(2) The final report on a significant incident must include:

- a detailed description of the incident
- the type of threat or root cause likely to have caused the incident
- the confirmed indicators of compromise
- the information about the suspected or confirmed cyber attacker
- the information about the severity and impact of the incident, which must include a description of the disruptions caused by the incident in the provision of services or the carrying out of the activities of the entity, the duration of the incident and the number of recipients of services affected by the incident, as well as any compromise of sensitive data
- the risk mitigation measures applied and the ongoing risk mitigation measures
- the measures to achieve a higher level of cybersecurity that the entity plans to apply to minimise the possibility of recurrence of the same or a similar incident and to mitigate the risk
- information on the cross-border impact of the incident, if the incident had such an impact
- information on the cross-sectoral impact of the incident, if the incident had such an impact.

Article 71

(1) If an incident is still ongoing, essential and important entities must submit a progress report to the competent CSIRT within the deadline under Article 70, paragraph 1 of this Regulation, instead of a final report on a significant incident.

(2) The progress report must include:
- an updated description of the basic characteristics of the incident, the initial assessment of the significant incident and other information submitted under Articles 67 to 69 of this Regulation
- the type of threat or root cause likely to have caused the incident
- the risk mitigation measures applied and the ongoing risk mitigation measures
- an assessment and explanation of the causes that led to the prolonged duration of the incident response.

(3) In the event of a significant incident lasting longer than 60 days from the date of submission of the initial notification of the significant incident, essential and important entities shall submit a progress report to the competent CSIRT every 30 days.

(4) In the cases under paragraphs 1 and 3 of this Article, essential and important entities shall submit to the competent CSIRT a final report on a significant incident no later than within 30 days from the last submitted progress report.

Article 72

(1) Notifications of significant incidents shall be submitted on the forms established by the general guidelines for the implementation of the obligation to notify significant incidents.

(2) The general guidelines under paragraph 1 of this Article shall be adopted jointly by the competent CSIRTs, with the subsequent consent of the central government authority for cybersecurity.

(3) The forms and general guidelines under paragraph 1 of this Article shall be developed taking into account ENISA's technical guidelines on the parameters for information for the purpose of notifying ENISA under Article 42, paragraph 2 of the Act.

(4) The competent CSIRTs, after obtaining the consent of the central government authority for cybersecurity to the general guidelines under paragraph 1 of this Article, shall publish the general guidelines on their websites.

Article 73

(1) Competent CSIRTs may adopt sectoral guidelines for the implementation of the obligation to notify significant incidents if there are sectoral specificities that are not covered by the general guidelines under Article 72 of this Regulation.

(2) The competent CSIRTs shall publish the sectoral guidelines under paragraph 1 of this Article on their websites.

Article 74

(1) Special guidelines shall be adopted on the implementation of the obligation of essential and important entities to submit notifications of significant incidents to law enforcement authorities in cases under Article 37, paragraph 3 of the Act.

(2) The guidelines under paragraph 1 of this Article shall be jointly adopted by the competent CSIRTs in cooperation with the law enforcement authorities.

(3) The competent CSIRTs shall publish the guidelines under paragraph 1 of this Article on their websites.

SECTION 3
ACTIONS OF THE COMPETENT CSIRT IN RESPONSE TO NOTIFICATIONS OF SIGNIFICANT INCIDENTS

Article 75

If the notification of a significant incident is not provided in accordance with Articles 66 to 72 of this Regulation, the competent CSIRT shall notify the entity thereof and set a deadline within which the entity is required to remedy the deficiencies, with a warning of the legal consequences following the Act if the entity fails to do so within the given deadline.

Article 76

(1) The competent CSIRT shall provide the entity with initial feedback on the incident without delay and no later than within 24 hours from the receipt of the early warning of a significant incident.

(2) In addition to the initial incident feedback, the competent CSIRT shall submit to the essential and important entity guidelines and operational advice on the implementation of possible incident mitigation measures if requested by the entity in the early warning of the significant incident or the initial notification of the significant incident in the cases under Article 68 of this Regulation.

(3) If an entity is called upon to remedy deficiencies in the submitted early warning of a significant incident in accordance with Article 75 of this Regulation, the deadline under paragraph 1 of this Article shall be counted from the submission of the corrected early warning of a significant incident.

(4) The deadlines under paragraphs 1 and 3 of this Article in the cases under Article 68 of this Regulation shall be calculated from the receipt of the initial notification of a significant incident.

Article 77

Upon receipt of the notification under Articles 67 to 71 of this Regulation, the competent CSIRT shall analyse and classify the incident according to the national taxonomy of incidents and, if circumstances allow, upon receipt of such a notification, provide essential and important entities with information relevant for the follow-up of the significant incident, in particular information that could contribute to the effective handling of the significant incident.

Article 78

The national taxonomy of incidents under Article 77 of this Regulation shall be adopted by the central government authority for cybersecurity at the proposal of the competent CSIRTs.

Article 79

(1) The competent CSIRT shall be involved in the process of resolving a significant incident at the request of an essential and important entity.

(2) Essential and important entities may submit the request under paragraph 1 of this Article within any of the phases of reporting of a significant incident under Article 65 of this Regulation, using the reporting forms under Article 72 of this Regulation.

(3) In the case referred to in paragraph 1 of this Article, essential and important entities shall provide the competent CSIRT with all information necessary for the effective resolution of a significant incident at its request.

(4) The submission of data under paragraph 3 of this Article shall not affect the implementation of the obligations of essential and important entities under Articles 65 to 72 of this Regulation.

Article 80

(1) Upon receipt of the notification under Articles 66 to 72 of this Regulation on significant incidents having a cross-border or cross-sectoral impact, the competent CSIRT shall, without delay and no later than within three days of receiving such a notification, submit to the competent authority for the implementation of cybersecurity requirements a report on the potential cross-border and cross-sectoral impact of the significant incident, with an assessment of the potential impact of the incident.

(2) When preparing the report under paragraph 1 of this Article, the competent CSIRT shall also consider the information about the significant incident provided to it by the single point of contact and the competent authority for implementing cybersecurity requirements.

Article 81

The competent authority for implementing cybersecurity requirements shall, without delay and no later than within three days from receipt of the report under Article 80, paragraph 1 of this Regulation, respond to the competent CSIRT regarding the assessment of the cross-border and cross-sectoral impact of the incident.

Article 82

(1) If it receives new data on a significant incident that have an impact on the previously provided incident impact assessment or when requested to do so by the competent authority for implementing cybersecurity requirements, the competent CSIRT shall prepare a new report on the cross-border and cross-sectoral impact of the significant incident, with a new assessment of the impact of the incident.

(2) In the case referred to in paragraph 1 of this Article, Articles 80 and 81 of this Regulation shall apply accordingly.

Article 83

The reports of the competent CSIRT under Articles 80 and 82 of this Regulation shall be submitted to the single point of contact no later than within three days of completion, and the observations of the competent authority under Article 81 of this Regulation shall be submitted to the single point of contact no later than within three days of receipt.

Article 84

In carrying out the tasks under Articles 75 to 83 of this Regulation, the competent CSIRT shall prioritise tasks according to the risk assessment.

CHAPTER II
NOTIFYING SERVICE RECIPIENTS OF SIGNIFICANT INCIDENTS AND SIGNIFICANT CYBER THREATS

Article 85

(1) Essential and important entities shall, without delay, and no later than within 72 hours from the moment of becoming aware of a significant incident, in a clear and easily verifiable manner, notify the recipients of their services who could be affected by such an incident of the significant incident.

(2) The notification under paragraph 1 of this Article must contain the following information on the significant incident:

- the type and brief description of the incident
- the cause of the incident
- the possible impact of the incident on the service
- the contact details of the entity
- the instructions on the actions of service recipients to mitigate the impact of the incident and compensation for the damage caused.

(3) If at the time of sending the notification under paragraph 1 of this Article, some of the information under paragraph 2 of this Article is not known to the essential and important entity, the entity shall submit the remaining information to the recipients of services that could be affected by such an incident no later than within 72 hours of sending the notification.

Article 86

(1) In the event of a significant cyber threat, essential and important entities shall inform the recipients of their services, which may be affected by such a threat, of any possible protection measures or legal remedies that they may use to prevent or compensate for the damage caused and, where appropriate, inform the recipients of their services of the significant cyber threat.

(2) Article 85 of this Regulation shall apply *mutatis mutandis* to notifying service recipients of significant cyber threats.

CHAPTER III
VOLUNTARY NOTIFICATIONS OF ESSENTIAL AND IMPORTANT ENTITIES

Article 87

(1) When voluntarily notifying other incidents under Article 39 of the Act, essential and important entities shall submit an incident notification to the competent CSIRT, which must include the following:

- date and time of becoming aware of the incident
- description of the technical characteristics of the incident, including the duration of the incident and the type of threat or root cause likely to have caused the incident
- indicators of compromise, if available
- information about the vulnerabilities that are being exploited
- information about the entity’s network and information system that was affected by the incident
- description of the disruptions caused by the incident in the provision of services or the carrying out of the activities of the entity and the number of recipients of the entity’s services and/or users of the entity’s network and information system affected by the incident

- the risk mitigation measures applied and the ongoing risk mitigation measures
- the entity's experience with similar incidents in the past
- information on whether the incident is suspected to have been caused by illegal or malicious activity.

(2) Essential and important entities may submit the notification under paragraph 1 of this Article to the competent CSIRT immediately upon becoming aware of the incident and no later than within 30 days from the moment of becoming aware of the incident, taking into account the severity of the incident and the extent of the information at the entity's disposal on the near miss.

(3) From the moment of notification of an incident until the expiry of the deadline for its submission under paragraph 2 of this Article, essential and important entities may submit to the competent CSIRT the updated information under paragraph 1 of this Article.

Article 88

(1) When voluntarily notifying cyber threats under Article 39 of the Act, essential and important entities must submit to the competent CSIRT a notification of a cyber threat which must include:
- date and time of becoming aware of the cyber threat
- description of the cyber threat and its current status
- information on the potential impact of the cyber threat on the entity's network and information systems and its users, including a description of the disruptions that the cyber threat could cause in the provision of services or the carrying out of the activities of the entity
- description of the measures applied to prevent the impact of the cyber threat on the entity's network and information systems.

(2) Essential and important entities may submit the notification under paragraph 1 of this Article to the competent CSIRT immediately upon becoming aware of the cyber threat and no later than within 30 days from the moment of becoming aware of the cyber threat, considering the severity of the cyber threat and the extent of the information at the entity's disposal on the cyber threat.

(3) From the moment of notification of a cyber threat until the expiry of the deadline for its submission under paragraph 2 of this Article, essential and important entities may submit to the competent CSIRT the updated information under paragraph 1 of this Article.

Article 89

(1) When voluntarily notifying about near misses under Article 39 of the Act, essential and important entities shall submit to the competent CSIRT a notification of the near miss, which must include:
- date and time of becoming aware of the near miss

- description of the technical characteristics of the near miss, including the type of threat or root cause that may have caused the incident
- indicators of compromise, if available
- information about the vulnerabilities attempted to be exploited
- information about the entity's network and information system that was exposed to the near miss
- information on the potential impact of the near miss on the entity's network and information systems and its users, including a description of the disruptions that the near miss could have caused in the provision of services or the carrying out of the activities of the entity
- the entity's experience with similar near misses in the past
- information on whether the near miss is suspected to have been caused by illegal or malicious activity.

(2) Essential and important entities may submit the notification under paragraph 1 of this Article to the competent CSIRT immediately upon becoming aware of the near miss and no later than within 30 days from the moment of becoming aware of the near miss, considering the severity of the near miss and the extent of the information at the entity's disposal on the near miss.

(3) From the moment of notification of a near miss until the expiry of the deadline for its submission under paragraph 2 of this Article, essential and important entities may submit to the competent CSIRT the updated information under paragraph 1 of this Article.

Article 90

(1) Notifications of incidents, cyber threats and near misses shall be submitted on the forms established by the guidelines for the implementation of voluntary notification.

(2) The guidelines under paragraph 1 of this Article shall be jointly adopted by the competent CSIRTs, with the subsequent consent of the central government authority for cybersecurity.

(3) The forms and guidelines under paragraph 1 of this Article shall be developed taking into account ENISA's technical guidelines on the parameters of the information for the purpose of notifying ENISA under Article 42, paragraph 2 of the Act.

(4) The competent CSIRTs, after obtaining the consent of the central government authority for cybersecurity for the adopted guidelines under paragraph 1 of this Article, shall publish the guidelines on their websites.

Article 91

(1) In relation to the notification under Articles 87 to 89 of this Regulation, the competent CSIRT shall provide recommendations and operational advice to the essential and important entity on the implementation of possible measures to mitigate and effectively address the incident, prevent the occurrence of the potential impact of the cyber threat and near miss, if requested by the entity in the submitted notification of an incident, cyber threat or near miss.

(2) Where the submitted information indicates that the reported event has the characteristics of a significant incident under Articles 59 to 62 of this Regulation, the competent

CSIRT shall notify the essential and important entity of the obligation to notify the significant incident in accordance with Articles 64 to 74 of this Regulation.

Article 92

(1) The competent CSIRT shall be involved in the process of resolving an incident notified under Article 87 of this Regulation if the entity has requested it in the submitted incident notification.

(2) Article 79, paragraph 3 of this Regulation shall apply *mutatis mutandis* in the case referred to in paragraph 1 of this Article.

Article 93

When carrying out the tasks under Articles 91 and 92 of this Regulation, the competent CSIRT shall prioritise tasks which were deemed to be of prime concern according to the risk assessment, and when processing notifications received from essential and important entities pursuant to Articles 37 and 39 of the Act, the competent CSIRT shall prioritise the processing of notifications of significant incidents.

CHAPTER IV
NATIONAL PLATFORM FOR THE COLLECTION, ANALYSIS AND EXCHANGE OF DATA ON CYBER THREATS AND INCIDENTS

Article 94

(1) Essential and important entities shall use the national platform for collecting, analysing and exchanging data on cyber threats and incidents (hereinafter: national platform) as the primary means of submitting notifications on:

- significant incidents in accordance with Article 37 of the Act and Articles 58 to 73 of this Regulation, and
- other incidents, near misses and cyber threats in accordance with Article 39 of the Act and Articles 87 to 90 of this Regulation.

(2) In exceptional cases when submission of notifications in accordance with paragraph 1 of this Article is not possible for justified reasons, essential and important entities shall submit the notifications under paragraph 1 of this Article through communication channels defined in the guidelines of the competent CSIRTs under Article 72, paragraph 1 and Article 90, paragraph 1 of this Regulation.

Article 95

(1) Essential and important entities shall acquire the status of an entity using the national platform on the day of the entity’s entry in the list of essential and important entities.

(2) In the notification regarding the performed classification of entities under Article 19, paragraph 1 of the Act, the competent authorities for the implementation of cybersecurity requirements shall notify the essential and important entity of the acquisition of the status of an entity using the national platform and the obligations arising therefrom for the entity under Articles 96 and 97 of this Regulation.

Article 96

(1) Within eight days of receipt of the notification under Article 95, paragraph 2 of this Regulation, essential and important entities shall appoint a person responsible for the administration of the entity's account on the national platform (hereinafter: administrator).

(2) Essential and important entities shall appoint an administrator from among their employees.

(3) Essential and important entities may appoint up to two administrators.

(4) The data on the designated administrators, including changes to the administrator or individual data on the designated administrators, shall be entered into the national platform by the essential and important entities following the instruction forming an integral part of the notification under Article 19, paragraph 1 of the Act.

Article 97

(1) Within eight days of receipt of the notification under Article 95, paragraph 2 of this Regulation, essential and important entities shall appoint persons authorised to conduct the notification under Articles 37 and 39 of the Act (hereinafter: users of the national platform).

(2) Essential and important entities may appoint users of the national platform from among their employees or employees of an external provider of related services within the entity, where the responsibility for implementing the notification under Articles 37 and 39 of the Act remains upon the essential and important entity.

(3) In the decision on the appointment of users of the national platform, essential and important entities shall determine the scope of their user rights by specifying:

- whether the person is responsible for notifying under Article 37 of the Act and/or for notifying under Article 39 of the Act
- the type of services or activities of the entity listed in Annexes I and II to the Act to which the appointment from subparagraph 1 of this paragraph relates.

(4) When determining the total number of users of the national platform, essential and important entities shall consider the size of the entity, its structure, the degree of exposure of the entity to risks and the likelihood of incidents occurring.

(5) The administrator may also be appointed as a user of the national platform.

Article 98

On the national platform, the administrator shall have the following powers for the entity for which it has been appointed:

- entering users of the national platform and their user rights
- updating the data on users of the national platform, and

- deactivating users of the national platform
- deactivating user rights.

Article 99

Based on the decision on the appointment of users of the national platform under Article 97 of this Regulation, within the framework of their user rights, the administrator on the national platform shall grant the users of the national platform of the entity for which it has been appointed the following powers:

- entering notifications of significant incidents under Article 37 of the Act and/or
- entering notifications of other incidents, cyber threats and near misses under Article 37 of the Act.

Article 100

(1) In the notification under Article 19, paragraph 3 of the Act, the competent authorities for the implementation of cybersecurity requirements shall notify the entity of the termination of the entity's status as the user of the national platform.

(2) The notification under paragraph 1 of this Article shall also be submitted by the competent authority for the implementation of cybersecurity requirements to CARNET, in order to deactivate the user accounts of the administrator and the user of the national platform for the entity to which the notification relates.

(3) CARNET shall deactivate user accounts no later than three days from the receipt of the notification under paragraph 1 of this Article.

Article 101

(1) Essential and important entities shall use the national platform following the terms and conditions of use of the national platform contained in the guidelines for the use of the national platform.

(2) The guidelines for the use of the national platform shall be adopted by CARNET after obtaining the opinions of the competent CSIRTs and competent authorities regarding the implementation of cybersecurity requirements.

(3) When determining and updating the terms and conditions of use of the national platform, CARNET shall consider the guidelines of the competent CSIRTs under Article 72, paragraph 1 and Article 90, paragraph 1 of this Regulation.

(4) The terms and conditions of use of the national platform shall determine, inter alia, the terms and conditions of use of the national platform in the cases referred to in Article 59, paragraph 3 of the Act, following the protocol on the conduct of the competent authorities concluded for the entity.

Article 102

(1) CARNET shall grant rights of access to the national platform to the competent authorities under Annex III to the Act and the single point of contact, and enable its use to the extent necessary for the implementation of their tasks prescribed by the Act, namely:

- to the competent authorities for the implementation of cybersecurity requirements for the purpose of carrying out the tasks under Article 59, paragraphs 1 to 5 and Articles 64 and 65 of the Act
- to the competent CSIRTs for the purpose of carrying out the tasks under Article 66 of the Act, and
- to the single point of contact for the purpose of carrying out the tasks under Articles 40 to 42 of the Act.

(2) The competent authorities listed in Annex III to the Act and the single point of contact are required to inform CARNET on:

- staff responsible for administering the accounts of the competent authority or the single point of contact on the national platform
- other staff of the competent authority or the single point of contact authorised to use the national platform
- the scope of user rights for persons under subparagraphs 1 and 2 of this paragraph.

(3) In the cases referred to in Article 94, paragraph 2 of this Regulation, the competent authorities under Annex III to the Act and the single point of contact shall have access to the submitted notifications from essential and important entities in accordance with the guidelines of the competent CSIRTs under Article 72, paragraph 1, and Article 90, paragraph 1 of this Regulation.

Article 103

(1) Data on a significant incident shall be kept on the national platform for 25 years from the date of submission of the final report on the significant incident under Article 70 of this Regulation.

(2) Data on other incidents, cyber threats, and near misses shall be kept on the national platform for 15 years from the date of submission of the notification under Articles 87 to 89 of this Regulation.

(3) Data on entities using the national platform, their administrators and users of the national platform shall be kept for 15 years from the date of deactivation of the entity's user account in accordance with Article 100 of this Regulation, provided that the retention periods for all significant incidents notified by the entity concerned to the competent CSIRT have expired within that period.

(4) The competent CSIRTs shall, according to the division of competences under Annex III of the Act, after the expiry of the retention periods under paragraphs 1 and 2 of this Article, delete data on significant incidents, other incidents, cyber threats and near misses kept on the national platform.

(5) After the expiry of the retention period under paragraph 3 of this Article, CARNET shall delete the data kept on the national platform concerning the entities that use the national platform, their administrators and users of the national platform.

PART SIX
IMPLEMENTATION OF INCIDENT AND CYBER THREAT NOTIFICATION AS A VOLUNTARY CYBER PROTECTION MECHANISM

Article 104

(1) Entities referred to in Article 47, paragraph 1 of this Regulation that intend to use the possibility of notification of incidents and cyber threats under Article 50, paragraph 2 of the Act, shall notify the competent CSIRT of such an intention.

(2) In the annex to the notification under paragraph 1 of this Article, the entity shall submit the statement of compliance under Article 35, paragraph 3 of the Act, which shall not be older than one year from the date of drawing up the notification under paragraph 1 of this Article.

Article 105

(1) Entities referred to in Article 47, paragraph 1 of this Regulation shall perform cybersecurity self-assessments at least once every two years, as long as they use the possibility of notification of incidents and cyber threats under Article 50, paragraph 2 of the Act, and shall submit the drawn up statements of compliance under Article 35, paragraph 3 of the Act to the competent CSIRT without delay and no later than within eight days from the date they are drawn up.

(2) The deadline referred to in paragraph 1 of this Article shall be calculated from the date of drawing up the statement of compliance submitted to the competent CSIRT under Article 104, paragraph 2 of this Regulation, or from the date of drawing up the statement of compliance submitted to the competent CSIRT under Article 35, paragraph 3 of the Act.

Article 106

A significant incident within the meaning of Article 50, paragraph 2 of the Act, of which the entities under Article 47, paragraph 1 of this Regulation voluntarily notify the competent CSIRT shall mean any incident that meets at least one of the criteria for the determination of significant incidents under Articles 58 to 62 of this Regulation, taking into account the criteria thresholds, when prescribed.

Article 107

(1) Articles 87 to 92 of this Regulation shall apply *mutatis mutandis* to the implementation of notification of significant incidents, other incidents, cyber threats and near misses based on Article 50, paragraph 2 of the Act.

(2) Entities referred to in Article 47, paragraph 1 of this Regulation shall submit notifications of significant incidents, other incidents, cyber threats and near misses exclusively through communication channels defined in the guidelines of the competent CSIRTs under Article 90, paragraph 1 of this Regulation.

Article 108

When processing notifications of significant incidents, other incidents, cyber threats, and near misses received under Articles 37, 39, and Article 50, paragraph 2 of the Act, the competent CSIRT shall prioritise the processing of notifications received under Articles 37 and 39 of the Act.

PART SEVEN
NATIONAL SYSTEM FOR DETECTING CYBER THREATS AND PROTECTING CYBERSPACE

Article 109

(1) Essential entities, important entities and other entities that are not categorised as essential or important entities may voluntarily implement a cyber protection measure by accessing the national system for detecting cyber threats and protecting cyberspace (hereinafter: national system) if the central government authority for cybersecurity has assessed the entity as critical within the meaning of Article 52, paragraph 1 of the Act.

(2) In order to conduct criticality assessments of entities within the meaning of Article 52, paragraph 1 of the Act and to decide on priorities in implementing a voluntary cyber protection measure for access to the national system, the central government authority for cybersecurity shall classify entities according to risk categories.

Article 110

(1) Assessment of the criticality of an entity within the meaning of Article 52, paragraph 1 of the Act shall be conducted based on a request for access to the national system submitted by the entity, or based on a proposal for access to the national system submitted by a state administration authority or a regulatory body competent for the entity's sector.

(2) Requests and proposals for access to the national system shall contain information on:

- services provided by the entity or activities carried out by the entity in relation to other providers of identical or equivalent services or activities in the Republic of Croatia
- network and information systems used by the entity in providing services or carrying out activities, and their exposure to cyber risks, dangers and threats
- how the entity's network and information systems are designed, managed and maintained, as well as the applicable relevant European and international standards and best security practices.

(3) In addition to the information in paragraph 2 of this Article, proposals for access to the national system shall also include the statement on the reasons for which the cyber protection measure of access to the national system is proposed for the entity.

(4) Requests and proposals for access to the national system shall be submitted to the central government authority for cybersecurity according to the instructions published on its website.

(5) The authority submitting the proposal for access to the national system shall also notify the entity for which the proposal has been submitted.

Article 111

(1) The central government authority for cybersecurity may, if necessary, request additional data on the entity's network and information systems from the entity for which the assessment is carried out to determine the entity's criticality for accessing the national system.

(2) The entity shall submit the requested data to the central government authority for cybersecurity in accordance with the instructions under Article 110, paragraph 4 of this Regulation.

Article 112

(1) Notwithstanding Article 109 of this Regulation, ministries shall implement a cyber protection measure of mandatory access to the national system.

(2) Notwithstanding Article 109 of this Regulation, other state administration authorities, state authorities, and legal persons with public authority are required to implement a cyber protection measure of mandatory access to the national system when the following criteria are met:

- the entity is categorised as an essential entity, or
- the entity has been assessed by the central government authority for cybersecurity as critical within the meaning of Article 52, paragraph 1 of the Act.

(3) The assessment of the criticality of the entities under paragraph 2, subparagraph 2 of this Article shall be carried out based on the proposal of the competent authority for the implementation of cybersecurity requirements for the public sector.

(4) The central government authority for cybersecurity shall notify the entity of the fulfilment of the criteria under paragraph 2, subparagraph 2 of this Article and of the obligation of accessing the national system.

Article 113

(1) Regardless of whether a cyber protection measure is implemented as mandatory or voluntary, access to the national system shall be carried out based on an agreement concluded between the central government authority for cybersecurity and the entity accessing the national system.

(2) The agreement referred to in paragraph 1 of this Article shall regulate:

- mutual rights and obligations of the central government authority and the entity accessing the national system
- mutual conditions of data protection and confidentiality
- maintenance and protection of software and tools of the national system
- technical and other conditions for accessing and using the national system.

(3) The agreements referred to in paragraph 2 of this Article shall be appropriately classified.

PART EIGHT
TRANSITIONAL AND FINAL PROVISIONS

Article 114

(1) The single point of contact shall adopt the guidelines referred to in Article 31, paragraph 1 of this Regulation within 90 days from the date of entry into force of this Regulation.

(2) The central government authority for cybersecurity shall adopt the guidelines referred to in Article 40 of this Regulation within 90 days from the date of entry into force of this Regulation.

(3) The central government authority for cybersecurity shall adopt the guidelines referred to in Article 45, paragraph 3 of this Regulation within six months from the date of entry into force of this Regulation.

(4) The central government authority for cybersecurity shall prepare a correlation overview of the measures referred to in Article 49 of this Regulation within six months from the date of entry into force of this Regulation.

(5) The central government authority for cybersecurity shall adopt the national taxonomy of incidents referred to in Article 77 of this Regulation within 90 days from the date of entry into force of this Regulation.

(6) The central state authority for performing tasks in the technical areas of information security shall adopt the guidelines referred to in Article 57 of this Regulation within six months from the date of entry into force of this Regulation.

(7) The competent CSIRTs shall adopt the guidelines referred to in Articles 72, 74 and 90 of this Regulation within 90 days from the date of entry into force of this Regulation.

(8) CARNET shall adopt the guidelines referred to in Article 101 of this Regulation within 90 days from the date of entry into force of this Regulation.

Article 115

On the day of entry into force of this Regulation, the Decision on measures and activities for increasing national capacities for a timely detection and protection against state-

sponsored cyberattacks, Advanced Persistent Threat (APT) campaigns and other cyber threats, CLASS: 022-03/21-04/91, Reg. No.: 50301-29/09-21-2, of 1 April 2021, shall cease to be valid.

Article 116

This Regulation shall enter into force on the eighth day after the day of its publication in the Official Gazette, with the exception of the provisions of Articles 104 and 105 of this Regulation, which shall enter into force on 1 January 2026.

CLASS: 022-03/24-03/108
REG. NO: 50301-29/23-24-5

Zagreb, 21 November 2024

SECRETARY GENERAL PRESIDENT

Ivona Ferenčić Andrej Plenković

ANNEX I

LIST OF ACTIVITY SECTORS[1]

A. LIST FOR ANNEX I TO THE ACT – SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	– Electricity entities
		– Distribution system operators
		– Transmission system operators
		– Electricity producers
		– Nominated electricity market operators
		– Market participants providing aggregation, demand response or energy storage services
		– Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b) District heating and cooling	– Operators of district heating or district cooling
	(c) Oil	– Operators of oil transmission pipelines
		– Operators of oil production, refining and treatment facilities, storage and transmission
		– Central stockholding entities
	(d) Gas	– Gas suppliers, including public service suppliers
		– Distribution system operators
		– Transmission system operators
		– Storage system operators
		– LNG system operators
		– Natural gas undertakings
		– Operators of natural gas refining and treatment facilities
	(e) Hydrogen	– Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	– Air carriers
		– Airport managing bodies, airports, including the core airports and entities operating ancillary installations contained within airports
		– Traffic management control operators providing air traffic control (ATC) services
	(b) Rail	– Infrastructure managers
		– Railway undertakings, including operators of service facilities

[1] Types of entities **marked with** * are entities that are also required to submit data on the categorisation of entities and to submit data for the purpose of maintaining a special registry of entities.

	(c) Water	– Inland, sea and coastal passenger and freight water transport companies, not including the individual vessels operated by those companies
		– Managing bodies of ports, including their port facilities, and entities operating works and equipment contained within ports
		– Operators of vessel traffic services (VTS)
	(d) Road	– Road authorities responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity
		– Operators of Intelligent Transport Systems
3. Banking		– Credit institutions
4. Financial market infrastructures		– Operators of trading venues
		– Central counterparties (CCPs)
5. Health		– Healthcare providers
		– Reference laboratories
		– Entities carrying out research and development activities of medicinal products
		– Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of the 2007 National Classification of Activities – NKD 2007. (Official Gazette, Nos 58/07 and 72/07)
		– Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list)
6. Water intended for human consumption		– Suppliers and distributors of water intended for human consumption, excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
7. Waste water		– Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water, excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity
8. Digital infrastructure		– Internet Exchange Point providers
		– **DNS service providers, excluding operators of root name servers***
		– ccTLD name registry*
		– Cloud computing service providers*
		– Data centre service providers*
		– Content delivery network providers*
		– Trust service providers
		– Providers of public electronic communications networks

		– Providers of publicly available electronic communications services
9. ICT service management (business-to-business)		**– Managed service providers***
		– Managed security service providers*
		– Information intermediaries as defined by the regulation governing the exchange of electronic invoices between undertakings
10. Public sector		– State administration authorities
		– Other state authorities and legal persons with public authority
		– Private and public entities that manage, develop or maintain the state information infrastructure in accordance with the law governing the state information infrastructure
		– Local and regional self-government units
11. Space		– Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

B. LIST FOR ANNEX II TO THE ACT – OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
1. Postal and courier services		– Postal service providers
		– Providers of courier services
2. Waste management		– Entities carrying out waste management, excluding entities for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		– Entities carrying out the manufacture of substances and the distribution of substances or mixtures
		– Entities carrying out the production of articles from substances or mixtures
4. Production, processing and distribution of food		– Food businesses which are engaged in wholesale distribution and industrial production and processing
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	– Entities manufacturing medical devices and entities manufacturing in vitro diagnostic medical devices, with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of the List for Annex I to the Act – Sectors of High Criticality

	(b) Manufacture of computer, electronic and optical products	– Manufacturers of computer, electronic and optical products
	(c) Manufacture of electrical equipment	– Manufacturers of electronic equipment
	(d) Manufacture of machinery and equipment n.e.c.	– Manufacturers of machinery and equipment n.e.c.
	(e) Manufacture of motor vehicles, trailers and semi-trailers	– Manufacturers of motor vehicles, trailers and semi-trailers
	(f) Manufacture of other transport equipment	– Manufacturers of other transport equipment
6. Digital providers		**–Providers of online marketplaces***
		– Providers of online search engines*
		– Providers of social networking services platforms*
7. Research		– Research organisations
8. Education system		– Private and public entities in the education system

C. LIST FOR ENTITIES NOT INCLUDED IN THE ANNEXES TO THE ACT

1. Critical entities – entities determined as critical entities under the law regulating the area of critical infrastructure.

2. Registrars[2] – entities that provide domain name registration services, i.e. a legal or natural person who performs an independent activity authorised for the registration and administration of .hr domains on behalf of the ccTLD name registry.

[2] Included in the list of activity sectors exclusively as entities required to submit data for maintaining a special registry of entities.

ANNEX II

CYBERSECURITY RISK-MANAGEMENT MEASURES

1. Commitment and accountability of persons responsible for implementing cybersecurity risk-management measures

Objective: The objective of the measure is to ensure that the persons responsible for the management of the measures under Article 29 of the Act (hereinafter: persons responsible for the management of measures) recognise cybersecurity as a key aspect of the entity's operations and actively participate in the management of cybersecurity, improving the entity's cybersecurity level through the integration of cybersecurity into strategic plans and operational decisions.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

1.1 Define and adopt a strategic cybersecurity policy act via the entity's management body, that defines the entity's objectives in cybersecurity matters, the cybersecurity risk-management measures that the entity shall apply, the organisational system and the distribution of roles, responsibilities and obligations, and that describes the entity's cybersecurity management processes. The entity shall conduct a review of the cybersecurity risk-management measures in place at least once a year and assess their effectiveness and, if necessary, update the strategic cybersecurity policy act

1.2 Ensure that all employees of the entity and relevant legal persons with whom the entity has a business relationship, such as its suppliers or service providers, are aware of the main strategic determinants of the cybersecurity policy that apply to them

1.3 Provide the necessary resources for the effective implementation of cybersecurity risk-management measures, including financial resources, technical tools, and human resources with the necessary expertise. To ensure continuity in the implementation of appropriate cybersecurity risk-management measures and to maintain a high level of their effectiveness, the entity shall assess the necessary resources at least once a year and, if necessary, adjust them

1.4 Establish, document, and maintain active cybersecurity roles and responsibilities according to the entity's size and network and information systems, and update established roles and responsibilities, as necessary. Given the size of the entity, cybersecurity roles may be assigned to persons within the entity with dedicated roles solely in cybersecurity matters (special roles) or they may be assigned to employees as part of their existing roles within the entity

1.5 Separate individual roles in cybersecurity matters that could result in a potential conflict of interest (e.g. separation of roles for carrying out risk assessments and roles for implementing measures)

1.6 Appoint a dedicated person operationally responsible for cybersecurity at the level of the entire entity and who is provided with adequate access to the persons responsible for the implementation of measures in the entity

1.7 Ensure annual reporting of persons responsible for implementing measures on the state of cybersecurity. These reports should include an analysis of established cybersecurity risk-management measures, identified cyber threats and risks, and recommendations for improving

the level of cybersecurity. Regular reporting should ensure that those responsible for the implementation of measures are informed and enable strategic decision-making to raise the level of cybersecurity

1.8 Define and ensure security metrics on the state of cybersecurity necessary for reporting of persons responsible for implementing measures within the entity, that is, define key security metrics that will enable precise monitoring of the state of cybersecurity. These metrics should include indicators that imply monitoring and data collection, such as the number and type of incidents, response times, and the percentage of compliance with the prescribed cybersecurity risk-management measures. Regular collection and analysis of these data should ensure quality reporting of persons responsible for the implementation of measures

1.9 Ensure that appropriate activities are undertaken to raise awareness among persons responsible for implementing cybersecurity measures, particularly in matters of cybersecurity risk management and the potential impact of those risks on the services provided by the entity or the activity it carries out. These activities include educational workshops, seminars, and other forms of education on current cyber threats, best cybersecurity practices, and the importance of taking proactive measures to manage cybersecurity risks. This subset of cybersecurity risk-management measures should ensure that the entity's management body is informed and continuously engaged in achieving and maintaining a high level of cybersecurity

1.10 Ensure adequate mechanisms for the participation of persons responsible for implementing measures in cybersecurity initiatives and promoting continuous cybersecurity improvement. These mechanisms include regular meetings, working groups, and committees dedicated to cybersecurity issues, as well as a transparent flow of information between the cybersecurity operations team and the entity's management body. This subset of cybersecurity risk-management measures should ensure the engagement of persons responsible for implementing measures in cybersecurity decision-making and prioritisation

1.11 Ensure adequate mechanisms for monitoring the main cybersecurity indicators in near real-time. These mechanisms include the implementation of advanced monitoring systems, automatic alarms and dashboards, which enable continuous monitoring and rapid detection of potential cyber threats. In this way, it is possible to react to incidents promptly and minimise the potential impacts of incidents.

Measures 1.1 to 1.11 apply in full to both the IT and OT parts of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure										
	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	1.11
basic	A	A	A	A	C	C	A	C	C	C	C
intermediate	A	A	A	A	A	A	A	A	A	C	C
advanced	A	A	A	A	A	A	A	A	A	A	C

2. Management of software and hardware assets

Objective: The objective of the measure is to establish a structured approach to the identification and classification of the software and hardware assets of the entity and to establish complete control and protection of the software and hardware assets of the entity during their use, storage, transport and ultimately deletion or destruction, i.e. management of the life cycle of software and hardware assets.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

2.1 The act adopted by the persons responsible for the management of measures shall define the rules and responsibilities for the management of software and hardware assets and establish the criteria for the establishment of an 'inventory of critical software and hardware assets' (hereinafter: inventory of critical assets). This includes creating and documenting details such as: who is responsible for the various aspects of asset management, how assets should be classified into critical and other assets, i.e. into multiple groups or categories in terms of their criticality for the entity's operations, and the procedures that are implemented for the regular monitoring and maintenance of assets. An entity may define several clearly identifiable groups or categories of assets according to their criticality (for example, 'infrastructure', 'business applications', 'support applications', 'test systems' or 'publicly available services', 'internal services' or 'production', 'test', 'development' or a combination of similar categories. Then, the entity shall determine by this act which groups or categories represent critical software and hardware assets, whereby it is possible to define only the category of critical software and hardware assets, which then must include: email servers, VPN devices, security devices, as well as other software and hardware according to the criticality assessment carried out by the entity. As part of this procedure, the entity shall define the criteria for establishing an inventory of critical assets (for example, all assets designated as 'infrastructure' or as 'business applications', or in the case of choosing the simultaneous use of several different categories, critical assets may be defined as 'all publicly available services', 'complete infrastructure' and 'all business applications in production'). For example, the classification of an entity's software and hardware assets may be based on requirements for the availability, authenticity, integrity and confidentiality of the asset, but it must take into account the risks to which the assets are exposed and the significance of the assets to the entity's operations (as in the previous examples), as the ultimate goal is not to classify the assets themselves, but to enable the entity to apply different measures for different categories of assets according to the different risk profile assessed by the entity

2.2 Create a detailed inventory of critical assets that contains all the necessary information for effective management and ensure that it is updated to a level that enables the effective operational management of assets and the implementation of adequate measures and controls. The level of detail of the critical asset inventory shall be appropriate to the entity's business needs, and the inventory shall include at least the following:

- a list of network and information systems used by the entity in providing services or carrying out activities
- a list of key elements of network and information systems that are assessed as critical to maintaining the entity's business continuity

- a unique identifier for each individual asset (e.g. inventory number, name or FQDN – Fully Qualified Domain Name)
- location of the assets
- responsible person and organisational unit of the entity or external service provider

2.3 Identify the entity's critical data, taking into account the requirements for availability, authenticity, integrity, and confidentiality of the data, as well as the risks to which the data are exposed and the importance of the data to the entity's operations. An entity may define several clearly identifiable groups or categories of critical data (for example, any data that constitute a trade secret, personal details, classified data, or other data that the entity assesses as critical due to its importance to the entity's operations)

2.4 Define the rules for the use of portable media for storing critical data, with which all employees should be familiar, and these rules should ensure the use of portable media exclusively for business purposes, prevent the execution of program code from portable media and ensure automatic checks for malware, and when necessary, the use of appropriate encryption

2.5 Determine whether critical software and hardware assets are used exclusively on the premises of the entity or are also used outside the premises of the entity, and define responsibilities for keeping, using and returning them when they are used outside the premises of the entity

2.6 Expand the inventory of critical assets with software and hardware assets of lower criticality, i.e. with other groups or categories of assets, for entities that classify assets according to point 2.1 into several groups of critical software and hardware assets, in order to increase the scope of risk assessment to assets that may affect the protection of critical assets and enabling the extension of the application of additional protection measures, depending on the classification of the criticality of assets (for example, expanding the categorisation with 'test systems', since they are publicly available to third parties involved in their development)

2.7 Establish the implementation of regular activities for the timely supplementing and updating of the critical asset inventory in such a way that: a) the update of the critical asset inventory is an integral part of the procurement process of new software and hardware assets, including procurement for the replacement of previously acquired assets, or b) it introduces adequate automation in a way that prevents the introduction of changes to the software and hardware assets without updating the critical asset inventory

2.8 Implement detailed procedures and adequate technical measures for the safe disposal and transport of assets containing critical data, utilising generally recognised and proven methods for the safe disposal or deletion of data from devices and media for data storage, and ensure measures are in place to protect devices and media for data storage during transport. One-time transport of equipment or media can be protected by compensatory measures, such as storing it in secure containers or performing extraordinary transport control, etc., whereas equipment intended for frequent transport or mobile devices of any type must have and use built-in, non-detachable protection mechanisms, such as encryption of storage media. If it is not possible to apply the technical measures described, the software and hardware assets or data may be taken

outside the entity's premises only after the appropriate approval of the persons responsible for the management of the measures

2.9 Implement mechanisms for the physical identification and labelling of physical assets for processing data based on their volume and prevalence, which may include real-time monitoring and asset control using automation, leveraging Internet of Things (IoT) and Radio Frequency Identification (RFID) technologies.

Measures 2.1 to 2.9 shall apply in full to both the IT and OT parts of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure								
	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9
basic	A	A	A	A	A	C	C	C	C
intermediate	A	A	A	A	A	A	A	C	C
advanced	A	A	A	A	A	A	A	A	A

3. Risk management

Objective: The objective of this measure is to establish an appropriate organisational framework for risk management, enabling the entity to identify and respond to all risks that threaten the security of its network and information systems, thereby posing a risk to the entity's operations.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

3.1 Develop, document, implement, and update on an annual basis a risk management process that includes a risk assessment (identification, analysis, and evaluation), determination of risk levels and criticality, methods of risk treatment, and identification of risk owners and their respective areas of responsibility. An entity shall document, communicate and make available to its employees, who are responsible for the entity's risk-related business segments, cybersecurity policies and instructions on basic procedures for identifying, analysing, assessing and processing risks, in particular for individual risks that may lead to disruptions in the availability, integrity, authenticity and confidentiality of the entity's network and information systems

3.2 Conduct a risk assessment of assets from the critical asset inventory based on the all-hazards approach principle and determining the level of each individual risk. Given that cyber threats can have different origins, a risk assessment should be based on an approach that includes all threats to software and hardware assets, including physical threats such as theft, fire, flood, natural phenomena, failures, outages of electronic communications infrastructure, power outages or unauthorised physical access and damage to property, but also includes all threats that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services. Particular attention should be given to the risks

associated with using third-party services. It is possible to use a risk assessment approach based on the described approach of identifying operational risks for assets from the entity's inventory (asset-based approach), as well as an approach based on scenarios and identifying sources of strategic risks for the entity's operations (event-based approach)

3.3 The identified risks shall be documented, and a response to these risks shall be defined, commensurate with their level and criticality, including the implementation of appropriate and proportionate technical, operational, and organisational risk management measures. As part of their risk assessment, entities should take and prioritise cybersecurity risk-management measures proportionate to the degree of exposure of their business to the risks and the likelihood of incidents occurring and the severity of their impact on the entity's operations, including the potential social and economic, or cross-sectoral or cross-border impact of those risks

3.4 Implement detailed methods for risk analysis, assessment and reporting. An entity shall ensure the regular reporting of identified risks, including any changes in risk assessments and proposed measures to mitigate or eliminate them. The reports shall be submitted to the relevant business segments within the entity in order to enable informed decision-making about the cybersecurity risk-management measures taken and the need to update the entity's strategic cybersecurity documents

3.5 Maintain a register of identified risks. This register should contain detailed information on all identified risks, including a description of the risk, an assessment of the likelihood and potential impact of the risk, and the current status and measures taken to address the risk. The register must be regularly updated to reflect newly identified risks and changes to existing risks. In addition, the entity shall ensure that all relevant business segments within the entity are informed about the content and changes in the register of identified risks in order to enable effective risk management and informed decision-making about the necessary cybersecurity risk-management measures

3.6 Ensure the implementation of a risk assessment when implementing solutions that increase the entity's network and information system's exposure to cyberattacks, expand existing risks, or introduce the use of previously unknown network and information systems architectures or protection measures within the entity. This assessment should include the identification of new threats and vulnerabilities arising from the implementation of new technologies or solutions, as well as an analysis of their potential impact on the entity's overall cybersecurity. Based on the assessment results, the entity shall take appropriate measures to mitigate the identified risks before implementing the solutions described in the introduction. All activities and results related to the risk assessment shall be documented and reviewed by the relevant persons in charge of the safety of the entity

3.7 Use advanced software tools to assess and monitor risks. These tools should enable a detailed analysis and assessment of cyber threats, identification of vulnerabilities, and real-time monitoring of incidents. Software tools shall be capable of automatically collecting and analysing relevant data, generating reports, and providing recommendations for mitigating or eliminating risks. The entity shall ensure that these tools are used and updated regularly to ensure their effectiveness in identifying and managing risks. The results obtained from the use of these tools must be integrated into the overall risk management process within the entity

3.8 Integrate risk management as part of the entity's business-level Enterprise Risk Management (ERM).

CONDITION: Measure 3.8 is binding on an entity that has risk management processes in place at the level of its operations, in which case risk management, as described in the subsets of Measure 3 (3.1 to 3.7), is carried out in an integrated manner as part of the entity's established business risk management process. If an entity does not have risk management procedures in place at the level of its operations, it shall establish Measure 3 (3.1 to 3.7) as a new business process.

Measures 3.1 to 3.8 shall apply in full to both the IT and OT parts of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure							
	3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8
basic	A	A	A	A	A	C	C	B
intermediate	A	A	A	A	A	A	C	B
advanced	A	A	A	A	A	A	C	B

4. Security of human resources and digital identities

Objective: The objective of this measure is to establish a structured approach that enables the entity to manage the recruitment of adequate human resources effectively and to manage the access rights of employees and external staff to the entity's network and information systems.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

4.1 Develop, document, implement and regularly maintain human resources security rules, taking into account all users of network and information systems, including external associates. Responsibilities related to cybersecurity shall be determined based on the assigned roles of the system users, as determined according to the entity's business needs. Entities shall ensure that:

- all employees of the entity understand their responsibilities in cybersecurity matters and apply basic cyber hygiene practices
- all persons with administrative or privileged access to the entity's network and information system are aware of the increased responsibility and are committed to fulfilling their roles and powers assigned under the entity's cybersecurity policy
- the persons responsible for managing the measures in the entity understand their roles, responsibilities and powers

4.2 Check the adequacy and qualifications of candidates before their employment according to the level of importance of the position to be filled and the applicable regulations (e.g., reference checks, validity check of certificates and diplomas, written tests, certificates of no criminal

record, etc.). It is necessary to determine the roles, responsibilities, and powers within the entity which require verifying the adequacy and qualifications of candidates before employment, i.e., which require, for example, the periodic submission of a certificate of no criminal record. The screening of candidates shall be carried out following applicable laws, regulations and ethics and shall be proportionate to business requirements, aligned with the requirements of access to certain types of data and identified risks

4.3 For all employees whose regular duties include designing, implementing, supervising or reviewing cybersecurity risk-management measures, provide specific and documented training immediately after the person enters into employment, as well as continuous training of all such existing employees during the employment relationship, in order to ensure an adequate level of knowledge on new technologies and cyber threats. The entity shall establish a training program in accordance with its cybersecurity policy, theme-specific policies, and relevant cybersecurity procedures within the entity's network and information system. The training shall include the necessary skills, expertise and knowledge for the specific positions, as well as the criteria against which the necessary training for each role is identified (for example, IT administrators shall receive additional training for secure configurations of the entity's software and hardware assets). The training program should include chapters such as:

- common and documented instructions relating to the secure configuration and operation of the entity's network and information systems, including mobile devices
- common and documented information on known cyber threats
- common and documented handling of the incident

4.4 Provide regular training on basic cyber hygiene practices and raise awareness of risks and cyber threats among all employees immediately upon their entry into employment with the entity and regularly thereafter during the employment relationship. The entity shall establish an awareness-raising program in accordance with its cybersecurity policy, theme-specific policies, and relevant cybersecurity procedures within the entity's network and information system. Awareness-raising shall include basic IT skills and knowledge (for example, all employees shall receive training in the safe use of email and internet browsing). An awareness-raising programme should include chapters such as:

- common and documented instructions related to the security of IT systems and personal IT assets, including mobile devices
- secure use of authentication methods and credentials (e.g., avoiding the use of the same passwords on different public services and avoiding the use of official addresses on public services to reduce the risk of attacks, avoiding saving passwords in web browsers, etc.)
- recognising and reporting the most common incidents

4.5 Define adequate disciplinary measures for employees in the event of non-compliance with relevant cybersecurity rules, depending on the employee's post, in accordance with the applicable legal framework. The determination of breaches of work obligations and the determination of disciplinary measures for violations of the entity's cybersecurity policies shall

take into account all applicable regulations, as well as specific contractual or other business requirements

4.6 Ensure that each user of the network and information system (whether or not they are an employee of the entity), wherever technically possible and the system allows, possesses one or more digital identities that are their own and uses them when working on the entity's network and information systems. If the system does not allow the creation of an adequate number of digital identities or it is unjustifiably costly, some users can use the same digital identities only if the entity provides a compensatory measure that ensures unambiguous and demonstrable records of the use of shared digital identities (for example, group use of an institutional email address). The entity shall:

- create unique digital identities for users and network and information systems
- for users, the digital identity must be linked to a unique person so that the person can be held accountable for the activities carried out with that specific identity
- enable the supervision of the digital identity system
- keep records of digital identities and ensure that all changes are monitored and documented
- digital identities assigned to multiple people (e.g., group email accounts) may only be permitted when necessary for business or operational reasons; they shall be specifically approved and documented, and a compensatory record-keeping measure shall be established that provides information on each individual user and the time of use of such digital identity

4.7 Define cybersecurity responsibilities according to clear job roles of employees and provide replacements for each role. Employee access rights to the entity's network and information systems should be implemented according to the assigned work duties and with the application of the principles of 'need-to-know', 'least privilege', and 'segregation of duties'

4.8 Ensure the implementation of a clear and efficient process for assigning in due time digital identities for all network and information system users and for changing or terminating them in due time in case of organisational or business changes. This process shall ensure that digital identities are assigned to new users in due time and that they are quickly terminated when no longer needed. Access rights shall be recorded and regularly revised and adjusted in line with organisational or business changes, minimising the risk of unauthorised access and protecting the entity's critical data

4.9 Develop and conduct incident response training within the entity for key persons involved in the process. Training shall include practical scenarios and regular exercises to ensure that all participants are well-prepared to effectively respond to incidents. By regularly updating the training, the entity shall adapt the training to new threats and best practices in the field of cybersecurity. This increases the entity's resilience to incidents and ensures a quick and adequate response in the event of their occurrence

4.10 Utilise remote digital learning systems for the continuous training and certification of staff in the field of cybersecurity, particularly in managing cybersecurity risks and their impact on the services provided or the activities carried out by the entity. An entity can also opt for remote

digital learning for the fact that it simplifies the provision of the training, regardless of whether it is possible to organise face-to-face training

4.11 Implement social engineering testing, phishing simulations and awareness-raising programmes. These activities must be regular and involve all employees of the entity in order to identify vulnerabilities and educate staff on how to identify and respond to such vulnerabilities. Awareness-raising programmes should include educational materials, workshops, and practical exercises. This strengthens the security culture within the entity and reduces the risk of successful social engineering attacks

4.12 Integrate the system for record-keeping and human resources management with the systems for managing digital identity and access rights of the network and information system to ensure the effective management of digital identities and access rights in real time. The entity shall:

- grant and revoke access rights based on the 'need-to-know' principle, the 'least privilege' principle and, as appropriate, the principle of 'segregation of duties'
- ensure that access rights are revised in the event of termination or other change of employment status (e.g., withdrawal or change of access rights, deactivation of user accounts, etc.)
- ensure that access rights are appropriately assigned to third parties, such as direct suppliers or service providers, taking into account the application of the principles set out in indent 1 of this subset of measures. It is particularly important to limit such access rights, both in scope and duration.
- maintain a register of access rights granted by users and
- utilise access logging to manage access rights in the network and information system.

The measures from 4.1 to 4.12 apply in full to both the IT and OT parts of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure											
	4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9	4.10	4.11	4.12
basic	A	A	A	A	A	A	A	A	C	C	C	C
intermediate	A	A	A	A	A	A	A	A	A	A	C	C
advanced	A	A	A	A	A	A	A	A	A	A	C	A

5. Basic practices of cyber hygiene

Objective: The objective of the measure is to ensure the implementation of basic security settings, rules and procedures for all employees and network and information systems of the entity and its data, with a focus on preventing the most common types of incidents that occur

as a result of malicious system infection, phishing attacks, improper and incorrect system configuration or the use of weak passwords.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

5.1 Develop, document, maintain and implement the rules of basic cyber hygiene practice and regularly educate all users of its network and information systems about these rules

5.2 Ensure that all network and information access systems that use passwords use 'the strongest possible passwords' as a means of authentication, or if this is not possible for operational reasons, the entity will define and explain its password policy, which must follow current good practices, such as the 'Password Policy Guide of the Center for Internet Security (CIS)'. If the entity has decided to implement its password policy, it should include different guidelines for different network and information systems and the purposes of password use, given that the level of necessary protection is often not the same for all types of network and information systems (for example, on newer Windows Server systems, using a password longer than 14 characters prevents the use of outdated LAN Manager authentication). In general, for all network and information systems that do not support multi-factor authentication (MFA) or for user accounts where MFA is not technically feasible, the minimum password length is 14 characters, which must include a combination of uppercase and lowercase letters, digits, and special characters. The password for user accounts with privileged access rights to the network and information system should be at least 16 characters long, and the password for service accounts should be at least 24 characters long, using the previously described rule for combining uppercase and lowercase letters, digits, and special characters. For user accounts, including those with privileged access rights and service accounts, for which two-factor verification is included, the password length may be shorter, but not shorter than 8 characters, if technically feasible, taking into account the need to use the rule of a combination of uppercase and lowercase letters, digits and special characters described above. If the network and information system cannot support the application of the described rules for determining passwords, the entity is required to provide other compensatory protection measures, i.e. restriction of access to the network and information system based on an appropriate compensatory measure (for example, mandatory restriction of physical access or mandatory remote access that is protected by two authentication factors). If the entity has opted for authentication that does not include the use of passwords, it is necessary to use two factors (biometrics and possession of another authentication device or a controlled access device). Under this subset of measures, the entity shall:

- ensure that the authentication strength is appropriate to the criticality of the network and information system and in accordance with the risk assessment
- use authentication methods (passwords, digital certificates, smart cards, biometrics, etc.) that are in line with developed technology and use unique authentication means (something that the user knows, such as a password or PIN, something that the user owns, such as a smartphone or token, and something that the user is, such as a fingerprint, facial recognition, etc.)
- ensure the secure allocation and use of authentication means (e.g., storage and transfer of such means in a protected form, automatic generation, creation of

cryptographic summaries with ‘salting’ and/or ‘peppering’, etc.), including advising staff on appropriate action
- request an initial change of personal access data (password and PIN) when using the user account for the first time, as well as in case of suspicion that personal access data have been compromised
- if technically feasible, it is necessary to prohibit saving passwords in web browsers
- ensure that user accounts are locked out after excessive failed login attempts (account lockout) with the possibility of automatic unlocking after a reasonable period to prevent denial-of-service attacks
- shut down inactive user sessions after a predetermined period of inactivity where the business process allows, and
- require special credentials to access privileged or administrator user accounts

5.3 In addition to implementing a password policy, implement multi-factor authentication (MFA) for critical network and information systems that are more exposed to potential cyberattacks. The application of MFA is required for VPN access, SaaS tools available on the internet, etc. It is necessary to ensure that usernames and passwords used on services with two-factor authentication are not used on other services without two-factor authentication. The authentication strength shall be consistent with the risk and exposure assessment of the network and information system. Multi-factor authentication must be considered when accessing critical network and information systems from a remote location, systems for administration of users and network and information systems, critical data of the entity, etc. Multi-factor authentication can be combined with other techniques to require additional factors in specific circumstances based on predefined rules and patterns, such as access from an unusual location, from an unusual device, or at an unusual time

5.4 Ensure the use of a basic antivirus tool on all workstations. The use of software antivirus tools for malware detection and recovery is often not enough, so following the risk assessment carried out by the entity, it is necessary to apply additional measures, i.e. use tools for detecting and responding to cyber threats on endpoints (EPP/EDR), with an appropriate level of automatic threat response, for advanced protection on all workstations and servers where technically feasible. An entity may, due to technical complexity or a very high cost of implementation, decide to apply the measure only to a selected and reasoned subset of software or hardware assets following the risk assessment, for example, on the server infrastructure, but then it must be logically separated from the unprotected software and hardware assets so that the compromise of unprotected software and hardware assets would not easily lead to the compromise of the protected part of the software and hardware assets

5.5 Ensure the timely and complete application of security patches on the complete software and hardware assets of the entity as soon as they are applicable, or it is necessary to elaborate, define, document and implement a different vulnerability management process on the network and information systems used, which will ensure triage, assessment and prioritised and documented gradual application of security patches. If an entity decides not to apply all security patches immediately but to implement its own security patch policy, the policy must take into account, when defining an internal deadline for the implementation of the security patches, the criticality and exposure factors of the network and information system, the severity of the detected vulnerabilities, i.e. criticality of the application of the security patch and the general

state of cybersecurity and any ongoing cyberattacks that exploit the vulnerabilities in question. In doing so, entities shall establish and apply procedures to ensure that:

- security patches are appropriately checked and tested before they are deployed in a production environment
- security patches are downloaded from trusted sources and checked for integrity
- security patches are not applied if they introduce additional vulnerabilities or instabilities that are more risky than the original reason for applying the patch
- the reasons for not applying the available security patches are documented
- in cases where a security patch is not available, additional cybersecurity risk-management measures are implemented, and the remaining risks are accepted
- the management of security patches is aligned with the control procedures for managing changes and maintaining network and information systems

5.6 Ensure, as far as technically feasible, the creation of a record of each report and activity in a critical network and information system to provide a forensic trail, using tools and processes to monitor and record activities in the entity's network and information system to detect suspicious events that could constitute an incident and acting to minimise the potential impact of the incident. Log entries shall be kept stored for at least the last 90 days (not necessarily in the system that created them). In exceptional cases, certain types of log entries may be retained for a shorter period if the volume of these records exceeds the storage limit, and it is not possible to filter and/or compress them to retain key information and reduce the number of records. As part of the regulation of the process of recording log entries (scope and period of retention), risk assessment should be taken into account to enable the detection and investigation of incidents in accordance with the assessed risk scenarios. The entity shall ensure that all systems have synchronised time so that log entries between different networks and information systems can be correlated. During the design of the network and information system, the following types of log entries should be included at a minimum:

- metadata of outgoing and incoming network traffic
- access to network and information systems, applications, network equipment and devices
- creating, modifying and deleting user accounts and extending rights
- changes to backup copies
- logs from security tools, such as an antivirus system, an attack detection system, or a firewall

5.7 Define and document the process of identifying and managing vulnerabilities in critical network and information systems that it develops independently. To this end, the entity shall provide a mechanism for identifying possible vulnerabilities in the network and information systems that it develops independently. According to an own risk assessment, the mechanisms may include static code analysis tools (SAST), dynamic application security testing tools (DAST), third-party component verification (SCA), internal or external penetration tests, inclusion in bug bounty programmes, or similar. It is recommended to apply the principle of shifting security checks 'to the left', i.e. to the earlier stages of software development. If the entity does not apply the above principles of shifting security checks 'to the left', then before putting a new or changed network and information system into production, it is necessary to conduct adequate security testing

CONDITION: Measure 5.7 is binding if the entity uses software solutions that it develops independently.

5.8 Implement mechanisms for periodic or regular vulnerability checks of all network and information systems to detect the lack of application of security patches or improper system configuration in due time. Entities are required, based on the risk assessment, to determine the need and frequency of this type of security testing (penetration tests, red teaming, purple teaming, etc.) to detect vulnerabilities in the implementation of the network and information system. The results of security testing and vulnerability check should be prioritised, used to improve the security of the network and information system, and monitored until they are resolved. Policies and procedures should be updated as necessary. An entity may limit this measure to critical software and hardware assets under Measure 2.1.

5.9 Ensure the central storage of security-relevant events using a copy of the log entries, continuously or at intervals not exceeding 24 hours, from the place where they were generated to a centralised system that allows storage and retrieval and where they are protected from unauthorised access and modification (if possible, the administrator of the source system should not be the administrator of this centralised system). Ensure that the central system can identify anomalies and potential incidents and generate alerts for suspicious events. Monitoring of log entries should take into account the importance of software and hardware assets, as well as risk assessment. It is necessary to generate a larger number, or it is allowed to generate a smaller number, of different types of warnings about suspicious events, taking into account risk scenarios and estimated risks. An entity shall verify at pre-planned intervals that log entries are recorded correctly through the performance or simulation of an action that should result in the recording of an appropriate log entry. The entity shall ensure that monitoring is also implemented in a manner that minimises the occurrence of false positives and false negatives

5.10 Ensure that controls are in place to prevent or detect the use of known or suspected malicious websites. The filter can be achieved by applying a list of prohibited categories or domain names or by applying a list of allowed categories or domain names, depending on the entity's risk appetite and business needs

5.11 Reduce the entity's potential exposure area to cyberattacks by:

- identification and restriction of services that are publicly exposed/available via the internet (e.g., websites, email, VPN entry points, monitoring consoles, RDP or SSH services for remote administration, SFTP, SMB and similar file-sharing services, etc.)
- reducing the number of administrator and highly privileged user accounts
- blocking access to publicly available services from the Tor network and known anonymisation VPN services
- restricting direct access to internet servers, if possible.

Measures 5.1 to 5.11 shall apply in full to the IT part of the entity's network and information systems. Points 5.1, 5.2, 5.3, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10 and 5.11 above shall apply to OT systems, while point 5.4 above shall apply, depending on the risk assessment of the implementation of such a measure on OT systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure										
	5.1	5.2	5.3	5.4	5.5	5.6	5.7	5.8	5.9	5.10	5.11
basic	A	A	A	A	A	A	C	A	C	C	C
intermediate	A	A	A	A	A	A	B	A	A	A	A
advanced	A	A	A	A	A	A	B	A	A	A	A

6. Ensuring network cybersecurity

Objective: The objective of the measure is to ensure the integrity, confidentiality and availability of the entity's network resources.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

6.1 Define and establish, following an own network architecture and exposure to public networks, mandatory network protection measures while considering adequate measures such as the use of firewalls, virtual private networks (VPNs), network access with the constant application of the principle of zero trust, secure network protocols for the wireless network, separation of networks for different purposes, according to the criticality of the data or the priority of individual network segments (e.g., office network, surveillance network, production, manufacture, guests, etc.)

6.2 Ensure that mandatory network protection measures ensure the secure transmission of critical data and the authorisation and control of use of networks and network-accessible resources. For example, the entity shall ensure the use of secure versions of protocols such as HTTPS and sFTP, network access only for authorised individuals or devices (authorisation may be based on the individual's verified digital identity, verified digital identity of the device, both, or where otherwise not possible, on the location of the connection if location access authorisation is performed, such as a guarded office space or data centre)

6.3 Conduct a comprehensive review of all defined network protection measures on an annual basis to ensure they remain effective and relevant. This review assesses current cyber threats, vulnerabilities, and changes in the business environment that may impact the existing protection measures. Based on the review's results, technical protection measures are updated to address new challenges and risks, ensuring continued compliance with best practices and requirements. Any results and changes proposed shall be documented and approved by persons responsible for implementing the measures

6.4 Implement mechanisms for monitoring both outgoing and incoming network traffic to reduce the risk of cyberattacks and define methods for filtering undesirable network traffic in terms of identifying potential indicators of compromise. This includes setting up appropriate tools for monitoring and analysing network traffic that allow for the identification and automatic blocking of potentially dangerous activities. Additionally, the entity shall define and

implement methods for filtering unwanted network traffic, including the use of intrusion detection and prevention systems (IDS/IPS) and other security solutions. All implemented filtering mechanisms and methods must be regularly reviewed and updated to maintain a high level of network security. This measure does not affect the prohibition of surveillance of electronic communications regulated by the law governing electronic communications

6.5 Implement technical mechanisms for detecting anomalies in the network based on either deviations from typical network traffic or deviations from internally defined rules.

Measures 6.1 to 6.5 apply in full to the IT part of the entity's network and information systems. The measures outlined in points 6.1, 6.3, and 6.5 above shall apply in full to the entity's OT systems.

Point 6.2 above is also applicable to the OT part of the entity's network and information systems, depending on the additional assessment of the criticality of the entity's data in the OT system environment, while point 6.4 above is applicable, depending on the assessment of the possible negative impact of automatic blocking of potentially dangerous activities on the operational performance and security of the OT system.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure				
	6.1	6.2	6.3	6.4	6.5
basic	A	A	A	C	C
intermediate	A	A	A	A	C
advanced	A	A	A	A	A

7. Control of physical and logical access to network and information systems

Objective: The objective of this measure is to establish a comprehensive system of policies and procedures to control physical and logical access to the entity's network and information systems, thereby preventing unauthorised access to the entity's software and hardware assets, and data.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

7.1 Develop, document, maintain and implement access control rules for the network and information system. Access control refers to all persons and external systems that access the entity's network and information systems. The access control policy and rules should include the elaboration of access control for:

- employees and staff of other entities representing direct suppliers or service providers
- processes within the network and information system of the entity that enable connection with other processes outside the network and information system of the entity.

The entity does not have to document access control rules if it exclusively uses cloud computing services; however, even in this case, it must ensure the life cycle management of the digital identities of all its users, as per Measure 4.6.

7.2 Ensure that owner roles are defined on applications that approve user rights association and provide records of who approved the assignment of rights. Access rights to network and information systems shall be granted, amended, revoked, and documented in accordance with the entity's access control policy. If access rights are defined through roles, each role must be associated with an owner. The role owner is responsible for assigning rights. An entity shall maintain records of the approval for the assignment of roles in accordance with the log entry recording and monitoring policy. An entity may decide to document or implement in its system for assigning rights to users the mapping of work roles to functional roles in individual network and information systems with the aim of faster and more efficient management of digital identities

7.3 Conduct regular checks of user access rights. Access rights shall be reviewed and documented at planned intervals, at least once a year, and adapted to the entity's organisational and business changes, and documented with adequate monitoring of changes. An entity may limit this measure to critical software and hardware assets under Measure 2.1.

7.4 Ensure supervision and control of access to critical network and information systems for privileged users. The entity shall adopt and apply policies, or rules for managing privileged and system administrator accounts. The rules shall include:

- creating of specific accounts that will be used exclusively for system administration activities, such as installation, configuration, management, and maintenance
- individualisation and limiting of administrative privileges as much as possible
- use of privileged and administrator accounts exclusively for connection to administration systems and not for use in other business activities of the entity
- use of identification, strong authentication (such as multi-factor authentication methods), and authorisation procedures for privileged and administrator accounts

7.5 Apply real-time, risk-based dynamic access control where possible and feasible using advanced tools

7.6 Use advanced analysis of user behaviour of network and information systems (UEBA) that recognises unusual or suspicious behaviour of users, or cases in which some irregularities go beyond the scope of normal everyday patterns or usage.

Measures 7.1 to 7.6 apply in full to both the IT and OT parts of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure					
	7.1	7.2	7.3	7.4	7.5	7.6
basic	A	A	A	A	C	C
intermediate	A	A	A	A	C	C
advanced	A	A	A	A	C	C

8. Supply chain security

Objective: The objective of the measure is to establish a clear and comprehensive policy for direct suppliers or service providers, in particular for critical supply chains of ICT services, ICT systems or ICT products to reduce the identified risks and minimise vulnerabilities and optimise the supply chain of the entity, which will result in a more stable operation and greater reliability of delivery of its products and services.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

8.1 Develop, maintain, document and implement supply chain security rules that include minimum requirements for certain types of direct suppliers and service providers, in particular those supplying entities with ICT services, ICT systems or ICT products, and a process for verifying the security of its direct suppliers and services offered concerning critical network and information systems. An entity shall establish these rules for its direct suppliers and service providers, including those involved in the supply chain of ICT services, ICT systems, or ICT products. Supply chain security rules outline roles, responsibilities, and powers, including security aspects, regarding the relationship between the entity and its direct suppliers or service providers. It is recommended that the entity define rules for different suppliers if security aspects differ, for example, rules for suppliers of equipment and software in a commercial offer that differ from the rules for suppliers of custom software or cloud computing service providers (e.g., mandatory SSO) or providers of network and information system maintenance services

8.2 Identify all its direct suppliers and service providers, including those in the supply chain of ICT services, ICT systems or ICT products, and assess the potential risks to the entity's network and information systems arising from these business relationships and, on that basis, establish and maintain a register of direct suppliers and service providers that includes:

- contact points for each of them, and in particular for those that have access to or manage the entity's critical software or hardware assets
- a list of services, systems or products that the entity procures directly from identified direct suppliers and service providers

8.3 Define security requirements for direct suppliers and service providers that align with the entity's cybersecurity policies in the business cooperation, procurement, or service level agreements (SLAs).

The security requirements should include the following:

- security clauses in contracts (e.g. confidentiality clauses)
- in the case of concluding contracts for the provision of managed services and managed security services, contracts for the provision of such services shall be

concluded exclusively with providers of such services that are categorised as essential or important entities in accordance with the Act (verification of the status of categorisation of managed service providers and managed security service providers is carried out through the central government authority for cybersecurity)

- provisions on the obligation of the direct supplier or service provider to notify the entity immediately upon becoming aware of incidents that may affect the entity
- provisions on the right to request a cybersecurity audit and/or the right to proof that a cybersecurity audit has been carried out, or the possession of appropriate equivalent certificates from the direct supplier
- provisions on the obligation to manage vulnerabilities, which includes the detection and remedying of vulnerabilities, as well as the notification of vulnerabilities that may affect the entity
- provisions on possible subcontracting and security requirements for subcontractors
- provisions on the obligations of the direct supplier or service provider upon expiry or termination of the contractual relationship (e.g. retrieval and removal/destruction/disposal of data).

Security requirements may include the following:

- provisions on skills and training required for employees of the direct supplier or service provider
- provisions on certificates or other authorisations required for employees of the direct supplier or service provider.

8.4 Monitor, review, evaluate and repeat the security verification process of critical supply chains of ICT services, ICT systems or ICT products at the time of each new contracting, or at least every two years, or following an incident related to the service, system or product in question, or following significant changes in security requirements or the state of cybersecurity. Any deviations identified during the audit and evaluation should be addressed through a risk assessment. The control of security requirements should cover all contractually defined security requirements

8.5 Define the criteria and security requirements for the selection and conclusion of contracts with direct suppliers or service providers, as well as the criteria for evaluating and monitoring the security of individual suppliers and service providers, in particular those belonging to the critical supply chain of ICT services, ICT systems or ICT products. The entity should seek to diversify its sources of supply to limit dependency on a single supplier or service provider, and consider the results of coordinated security risk assessments of critical supply chains of ICT services, ICT systems or ICT products carried out by the Cooperation Group together with the European Commission and ENISA, where available. When defining the criteria and security requirements for the selection and conclusion of contracts, the entity shall take into account:

- the ability of the supplier and the service provider to ensure the implementation of the entity’s security requirements

- its own risks and the level of criticality of individual ICT services, ICT systems or ICT products that it procures, including the risk tolerance of suppliers or service providers

8.6 Develop incident response plans involving critical suppliers and service providers, particularly those belonging to the critical supply chain of ICT services, ICT systems, or ICT products. The entity shall develop incident response plans in accordance with documented procedures and within a reasonable time frame. Incident response must also include the activities of critical suppliers and service providers.

Measures 8.1 to 8.6 apply in full to both the IT and OT parts of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure					
	8.1	8.2	8.3	8.4	8.5	8.6
basic	A	A	A	A	C	C
intermediate	A	A	A	A	A	A
advanced	A	A	A	A	A	A

9. Security in the development and maintenance of network and information systems

Objective: The objective of this measure is to ensure that entities establish, document, implement, and continuously monitor the configuration of their network and information systems, including the security settings of hardware and software assets, as well as the external services and networks they use.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

9.1 Conduct an analysis of security requirements in the phases of drafting a technical specification, design or procurement of network and information systems, and define criteria for accepting solutions following defined security requirements

9.2 Establish, document, implement and continuously monitor the configuration of its network and information systems, including security configuration settings for all hardware and software assets, as well as for all external services and networks used throughout their life cycle

9.3 Prescribe procedures for managing changes as part of the maintenance of network and information systems, which shall include all software and hardware support used and changes to their configuration. The procedures are applied during the release into the production environment, during all planned or unplanned changes to software and hardware assets, or during any significant change in the configuration of network and information systems, as well as during the development process. Control procedures shall be prescribed as part of the entity's cybersecurity policies and should be made known to all relevant employees of the entity. In the event of urgent changes, it is necessary to document the results of the change and provide an explanation as to why the regular change procedure could not be followed, as well as the consequences that would have occurred if the regular change procedure had been implemented.

Tests that were not carried out due to urgent changes should be conducted at a later date. Whenever possible, changes should be tested and validated before they are rolled out into the production environment. Control procedures should include:

- change request
- change risk assessment
- criteria for categorisation and prioritisation of changes and associated requirements for the type and scope of testing to be carried out and the approvals to be obtained
- requests for the implementation of a reverse procedure for a return to the status quo ante
- documentation on the change and approval of the change, including data on the persons responsible for each segment of the network and information system

9.4 Develop, maintain, and implement security rules in the processes of developing and maintaining network and information systems. The entity shall provide mechanisms for ensuring a secure design (secure by design and by default) and a zero-trust architecture, identification of possible vulnerabilities in network and information systems that it develops, integrates, or implements independently, as well as define security requirements for development environments. Identification of possible vulnerabilities can be achieved during the early stages of design using the threat modelling methods, during development using various static (SAST) and dynamic (DAST) testing techniques, or after the development is completed using various types of testing of the final product or system (e.g. penetration testing). It is recommended to apply the principle of shifting security checks 'to the left', i.e. to the earlier stages of software development. The results of the safety testing carried out should be properly managed, as with any other risk

CONDITION: Measure 9.4 is binding on entities that independently develop or maintain network and information systems.

9.5 Provide continuous training to employees involved in the development of network and information systems, define internal standards for the secure development of network and information systems, and conduct regular code security reviews. The measure can be implemented by applying some of the collaborative development methods (pair programming, two pairs of eyes when accepting code changes, testing-based development, etc.), using static code analysis tools (SAST) and the like. Training employees involved in the development of network and information systems shall at least include:

- analysis of security requirements in the phases of development of technical specifications and design or procurement of network and information systems
- principles for designing secure systems and principles of secure software coding, such as the incorporation of system security measures in the design phase (security-by-design), threat modelling or a zero-trust architecture
- compliance with security requirements for development environments
- use of security testing as part of the development life cycle

CONDITION: Measure 9.5 is binding on entities that independently develop or maintain network and information systems.

9.6 Integrate security tools and processes into development operations and practices (DevOps, DevSecOps), or ensure security verification within the continuous integration and delivery (CI/CD) process. Entities must establish, document, implement and continuously monitor the configuration of their network and information systems, including the security configuration settings of hardware and software assets, which includes the application within the methodology of the continuous integration and continuous delivery process, following the selected practice.

Measures 9.1 to 9.6 apply in full to both the IT and OT parts of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of measures					
	9.1	9.2	9.3	9.4	9.5	9.6
basic	A	A	A	C	C	C
intermediate	A	A	A	B	B	C
advanced	A	A	A	B	B	C

10. Cryptography

Objective: The objective of this measure is for entities to establish comprehensive cryptographic policies and procedures tailored to their specific business needs, ensuring the protection of data in transit and at rest. The implementation of cryptographic policies should ensure the application of appropriate cryptographic techniques and algorithms, in accordance with best practices and regulatory requirements.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

10.1 Develop, document, maintain and implement rules for the application of cryptography in the entity to ensure the appropriate and effective use of cryptography for protecting the availability, authenticity, integrity and confidentiality of critical data according to the type of data and the results of the risk assessment

10.2 Use encryption methods to protect critical data in transit. Cryptographic algorithms, pre-encryption padding methods and key sizes for individual algorithms should be adapted to current good practices and shall be proportionate to the risk and need for protection of the entity

10.3 Ensure the secure management of cryptographic keys, which includes protecting them against unauthorised access. The entity shall define and document the rules of access to cryptographic key management, including methods for:

- key generation for various cryptographic systems and applications
- issuing and obtaining certificates with public keys
- distribution of keys to end users, including rules for the activation of received keys
- storing keys, including key access rules by authorised users

- the replacement or updating of keys, including rules on how and when the keys are exchanged
- handling compromised keys
- revocation of keys, including rules on how to revoke or deactivate keys
- recovery of keys that have been lost or damaged
- backup storage or archiving of keys
- destruction of keys
- recording and monitoring activities related to key management
- determining the validity period of keys

10.4 Implement encryption methods to protect critical data at rest. According to the criticality of the data, the entity will implement methods to protect critical data at rest. The methods shall cover all media on which the data in question is stored at rest. Cryptographic algorithms, pre-encryption padding methods and key sizes for individual algorithms should be adapted to current good practices and shall be proportionate to the assessed risk and need for protection of the entity

10.5 Conduct regular audits and updates of cryptographic policies and procedures. The rules of cryptographic policy and procedures are required to be updated at planned intervals and following the latest achievements in cryptography

10.6 Following the assessed risk, use quantum-resistant cryptography to protect against future threats where possible.

Measures 10.1 to 10.6 shall apply to the entity's critical data under Measure 2.3 and in accordance with the entity's risk assessment, regardless of whether the data is located on the IT or OT part of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure					
	10.1	10.2	10.3	10.4	10.5	10.6
basic	A	A	A	A	C	C
intermediate	A	A	A	A	A	C
advanced	A	A	A	A	A	C

11. Incident handling

Objective: The objective of this measure is to establish a comprehensive framework for determining the roles, responsibilities, and procedures that will enable the entity to effectively prevent, detect, analyse, contain, and respond to incidents, as well as recover from them.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

11.1 Develop and document procedures for incident handling, including defining roles, responsibilities and procedures for monitoring, preventing, detecting, analysing, containing and

responding to an incident, recovering from an incident, and recording and reporting incidents internally within clearly defined time frames

11.2 Establish basic procedures for the handling of incidents that require the entity to ensure, as a minimum, the following:

- establishing effective communication plans, including plans for incident classification according to the national taxonomy, internal escalation and incident reporting. In doing so, the entity shall, following the risk assessment, include in its communication plans rules for the use of multi-factor authentication or continuous authentication solutions, protected voice, video and text communications, and secure emergency communication systems.
- assigning incident detection and response roles to competent employees
- rules for dealing with documentation that will be used or created during the handling of the incident, which may include incident response manuals, escalation graphs, contact lists and forms to be completed and submitted to the competent authorities
- introducing a simple mechanism that allows the entity's employees and its direct suppliers and service providers to report suspicious events that could constitute an incident
- it is necessary to assess the impact of each individual incident on the entity's business continuity and appropriately establish an interface between the handling of incidents and the management of the entity's business continuity
- incident logging
- monitoring all elements necessary for the identification and monitoring of significant incidents and timely notification of significant incidents to the competent CSIRT, in accordance with the entity's prescribed obligations

11.3 Provide basic training for employees to identify and report suspicious events and incidents, which shall be repeated at least once a year for all employees. The implementation of the training shall be documented. The implementation of the training shall be adapted to the entity's business needs

11.4 Develop and document detailed procedures for monitoring, analysing and responding to incidents, taking into account a defined time frame for internal incident reporting. An entity shall define and document rules for triaging suspicious events, which determine the order in which such occurrences will be assessed and processed. In the triage process, when assessing a particular suspicious event, it is possible to estimate that a particular suspicious event is likely to be a false positive event or that the potential impact of such an event is likely to be less than expected, which can then reduce the priority for further assessment and processing of that suspicious event, i.e. an assessment of other suspicious events may be carried out before the final processing and assessment of that event is completed. An entity shall define procedures for incident containment, incident response, and incident recovery to prevent the incident, its recurrence, and spread and to eliminate its consequences. An entity shall define procedures for notifying the competent CSIRT of significant incidents, as well as for notifying relevant internal and external users of its network and information systems, in accordance with the defined communication plan and the entity's prescribed obligations

11.5 Conduct annual exercises in handling simulated incidents to verify the effectiveness of established procedures for monitoring, analysis, and response to incidents. The entity shall document the conduct of the exercises in the same manner as actual incidents, with a clear note in the documentation generated as part of the exercise implementation that it is not a real incident but an exercise. These can be red teaming exercises, tabletop simulation exercises, and purple teaming/adversary emulation & detection engineering exercises

11.6 Use specialised tools for automated detection and response to incidents (IDR/EDR/XDR/NDR). These tools shall be adequately integrated and connected to other security controls. As the number of suspicious events can be large, it is important that the entity does not find itself in a situation where it does not recognise key information indicating that a significant incident has occurred from a large number of suspicious events. It is more important for the entity to process and assess a smaller number of key suspicious events than to process and assess a larger number of all other suspicious events. That is why each suspicious event shall have an appropriate level of priority, based on which the triage process will determine the order in which suspicious events will be processed.

Measures 11.1 to 11.5 apply in full to both the IT and OT parts of the entity's network and information systems, while point 11.6 above is applicable depending on the assessment of the potential negative impact of automated detection and response to incidents on the operational impact and security of the OT system.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure					
	11.1	11.2	11.3	11.4	11.5	11.6
basic	A	A	A	A	C	C
intermediate	A	A	A	A	A	A
advanced	A	A	A	A	A	A

12. Business continuity and cyber crisis management

Objective: The objective of this measure is to ensure the existence of pre-prepared plans to minimise business interruptions and maintain the continuity of the entity's key business activities in the event of incidents and cyber crises.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

12.1 Develop, maintain and implement business continuity and cyber crisis management policies, which will identify the entity's key business activities and the organisational and technical prerequisites for their implementation as a basis for developing plans for a possible reduced scope of operations during incident recovery and return to normal business operations within a defined time frame and scope of operations acceptable to the entity

12.2 Conduct a Business Impact Analysis (BIA) that will identify critical business functions and risk assessment as a prerequisite for the development of incident recovery plans. Based on the results of that risk analysis and assessment, an entity shall, as a minimum, establish:

- Recovery Time Objectives (RTOs) to determine the maximum time that can elapse for the recovery of business resources and functions after an interruption in the operation of individual segments of network and information systems
- Recovery Point Objectives (RPOs) to determine the amount of data that can be lost per individual business activity carried out using a network and information system, or using ICT services and ICT processes that may be interrupted
- Service Delivery Objectives (SDOs) to determine the minimum level of performance to be achieved in order to enable business to carry on during alternative modes of operation
- RPOs, RTOs and SDOs shall be taken into account when establishing backup and redundancy policies. Likewise, RPOs, RTOs and SDOs shall be taken into account in the management of supply chain security, as well as in the security of the procurement, development and maintenance of network and information systems, including the elimination of vulnerabilities and their detection
- a list of key utilities required for the normal operation of network and information systems

12.3 Establish processes for managing cyber crises or large-scale cybersecurity incidents, ensuring that cyber crisis management processes address at least:

- the roles and responsibilities of the entity's employees to ensure that all employees are aware of their roles in crisis situations, including the specific steps to be followed
- appropriate communication measures between the entity and the relevant competent authorities following the National Cyber Crisis Management Programme
- maintaining the established level of cybersecurity of the entity in crises through the application of appropriate measures, such as systems and processes for support and establishment of possible additional capacities
- implementation of processes for the management and use of information received from the competent CSIRT or other competent authority related to incidents, vulnerabilities, cyber threats and necessary cybersecurity risk-management measures

12.4 Develop detailed plans for disaster recovery (DRP) and business continuity (BCP). Based on the results of the risk assessment and the business continuity plan, the entity's data backup and redundancy plan shall be developed, maintained and documented and shall take into account at least the following:

- recovery time
- ensuring that backup copies or redundant systems are complete and function correctly, including configuration data and data stored in the cloud computing environment
- storage of (online and offline) backups and redundant systems in a secure location or locations which are not on the same network as the primary system and are at a sufficient distance to avoid any disaster damage at the main location

- applying appropriate physical controls (such as restricting access) and logical controls (such as encryption) to backup copies, according to the level of criticality of the data in those copies
- restoring backup data or activating the switchover to redundant systems, including the approval process
- dependence on key utilities
- a roadmap of recovery activities related to the timing and interdependencies of individual recovery activities

12.5 Conduct testing of business continuity plans at least once a year. Business continuity plans shall be tested through exercises and reviewed periodically following incidents, changes in operations or assessed risks. The implementation of business continuity plan testing shall be documented to clearly identify the necessary improvements observed during testing. When testing a business continuity plan, the following should be tested:

- roles and responsibilities
- key contacts, i.e. contacts of employees with the necessary responsibilities, powers and competencies
- internal and external communication channels
- conditions for activating and deactivating the plan
- the order of action in recovery
- recovery plan for specific operations
- required resources, including backups and redundancies
- minimal restoration time (recovery), and depending on the plans, the resumption of activities (restore) after temporary measures
- connection with incident handling
- network and information systems, such as hardware, software, services, data, etc. (such as redundant network devices, servers located behind load distribution systems, disk RAID arrays, backup services, and multiple data centres)
- assets, including facilities, equipment and supplies
- use of alternative and redundant power sources

12.6 Conduct cyber crisis management exercises to test the entity's resilience to situations that cannot be predicted and planned, taking into account:

- roles and responsibilities of employees to ensure that all employees are aware of their roles in crisis situations, including the specific steps to be followed
- appropriate communication arrangements between the entity and the relevant competent authorities
- maintaining the established level of cybersecurity in crises through the application of appropriate measures, such as systems and processes for support and the establishment of additional capacities

CONDITION: Measure 12.6 is implemented as binding at the request of the competent authorities as part of implementing cyber crisis management exercises.

12.7 Implement redundancy for critical network and information systems, as well as critical data. In the process of implementation, the entity shall consider options to invest in its own

redundancy or engage a third party to provide the necessary redundancy and document this. Redundancy needs to be considered partially or fully for:

- network and information systems, such as hardware, software, services, data, etc. (such as redundant network devices, servers located behind load distribution systems, disk RAID arrays, backup services, and multiple data centres)
- assets, including facilities, equipment and supplies
- employees with the necessary responsibilities, powers and competencies
- appropriate communication channels
- key utilities

12.8 Use redundant data centres in locations where the probability of the same geographical location threats occurring is lower. The entity shall conduct a geographical location risk assessment using available data (for example, earthquake zones). The risk assessment shall be documented. Based on the risk assessment, it is necessary to define and implement the selection and use of different data centres, taking into account the legal regulations in force. The entity may conduct an analysis to determine whether the cost of using the redundant data centre exceeds the potential losses in the event of its non-use. In this case, the persons responsible for managing the measures can accept the risk based on the risk management process.

Measures 12.1 to 12.8 apply in full to both the IT and OT parts of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure							
	12.1	12.2	12.3	12.4	12.5	12.6	12.7	12.8
basic	A	A	A	A	C	B	C	C
intermediate	A	A	A	A	A	B	A	C
advanced	A	A	A	A	A	B	A	A

13. Physical security

Objective: The objective is to establish measures to prevent and monitor unauthorised physical access to the entity's network and information systems, thereby protecting these systems from possible damage and interference caused by physical threats.

As part of the implementation of this measure, the entity will implement the following subsets of measures:

13.1 Develop and implement a physical security policy that addresses the risks within its ecosystem. The policy should at least specify the scope of application, the levels of protection of individual spaces, the methods of application, the responsible persons and the regularity of checking the effectiveness of the measures. The policy, as well as changes to the policy, shall be communicated to all employees and relevant legal persons with which the entity has a business relationship

13.2 Provide basic physical safeguards such as adequate physical barriers, locks, security cameras and access controls. For defined security perimeters in which network and information systems and other related equipment are located, technical protection shall be put in place to ensure access to the premises depending on the risk assessment of the entity, taking into account the potential criticality of the network and information system and the criticality of the software and hardware assets located in that space

13.3 Regularly review and update security protocols for physical locations. To reduce risks, it is necessary to establish security protocols to prevent unauthorised access to critical network and information systems. Security protocols shall monitor the criticality of the network and information systems to which they apply

13.4 Implement more advanced physical protection measures that ensure clear access records and can be used for subsequent digital forensics. The entity shall implement more advanced physical protection measures according to its risk assessment and in terms of enabling the exchange of data with other monitoring systems (records management system) to be able to unambiguously store access data and enable analysis during the monitoring or incident

13.5 According to the entity's risk assessment, implement real-time monitoring of the critical software and hardware asset area.

Measures 13.1 to 13.5 apply in full to both the IT and OT parts of the entity's network and information systems.

Distribution of subsets of measures by levels of cybersecurity risk-management measures under Article 42 of this Regulation:

Level	Subsets of the measure				
	13.1	13.2	13.3	13.4	13.5
basic	A	A	A	C	C
intermediate	A	A	A	A	C
advanced	A	A	A	A	A

ANNEX III

SPECIFIC PHYSICAL SECURITY MEASURES FOR ENTITIES IN THE DIGITAL INFRASTRUCTURE SECTOR

Objective: The objective of these measures is to prevent and monitor the possibility of unauthorised physical access to the perimeter and facilities in which the network and information systems used by entities from the digital infrastructure sector under Annex I to the Act are located, as well as to prevent possible damage and disruption to their network and information systems, caused by intentional, unintentional and natural physical threats.

Essential and important entities from the digital infrastructure sector under Annex I to the Act are required to implement the following physical security measures:

1. Develop a physical security plan, which shall include:
   - a physical security risk assessment as part of the risk assessment carried out by the entity in the implementation of the measure 'Risk management' under Annex II, point 3 of this Regulation
   - determining the premises of the entity that need to be protected and determining the level of physical security that needs to be ensured for each such location, taking into account the specifics of the premises where the network and information systems are located
   - selection of physical security measures for the outer perimeter, facilities and premises where the entity's critical network and information systems are located
   - a list of access rights to facilities and premises under indent 2 of this point and the obligations and responsibilities of the entity's employees, security personnel, external associates and visitors
   - a plan for conducting periodic physical safety testing, taking into account that it must be carried out at least once a year as part of the risk assessment under indent 1 of this point
   - the manner of carrying out regular maintenance of the physical security system.

   In addition, concerning each of the premises with a different level of required physical security, the physical security plan shall set out the following elements of physical security:
   - control of access of persons, access authorisations of employees, security personnel, external associates and visitors to a particular area
   - equipment for the implementation of physical security measures that is installed at a particular location
   - action plan for security personnel or external intervention teams concerning a particular location.

2. Implement multiple physical security measures at each protected location. By introducing multiple physical security measures, it is necessary to ensure that they complement each other, whereby several systems of the same or similar purpose can be installed, all aimed at reducing the likelihood of physical threats materialising. The establishment of multiple measures involves determining the location to be protected, identifying the outer perimeter, the perimeter of the facility, and the perimeters of individual areas within the facility, each with a different level of physical security. External physical security measures shall be applied to the outer perimeter, defining the boundaries of the external space to be protected and deterring unauthorised access. The physical security measures applied within the protected area shall ensure that any unauthorised access attempts are identified and security personnel are simultaneously informed thereof, as well as that records of all access to these areas are stored. Physical security measures established closest to the premises where the network and information systems of the entity are located, shall further slow down or prevent unauthorised access until the arrival of security personnel or intervention teams at the site. These measures shall also provide records of the stay of authorised persons in a particular area in case of investigation.

3. It is necessary to physically clearly separate the space constituting the outer perimeter under the control of the entity from the public area or other area with which it borders. Clear warnings prohibiting entry for unauthorised persons shall be posted on the outer perimeter. The entity shall provide access through the outer perimeter for vehicles and persons, establishing separate areas for the delivery of equipment and the entry of external associates and other visitors. The internal areas of the facility where the entity's network and information systems are located shall be appropriately divided into areas where external associates and other visitors can enter and areas that are exclusively intended for the use of employees or only for a specific category of employees. The entry of vehicles, external associates, and other visitors shall be subject to appropriate control measures and comply with the entity's rules regarding the possibility of bringing technical equipment from external associates and visitors, or private technical equipment from the entity's employees, into certain premises with a different level of physical security.

4. Implement access control using mechanical, electronic, or procedural methods or a combination of these methods. Mechanical access control should be based on the use of security locks and security keys on the doors of protected areas. Electronic access control should be based on the use of an automatic access control system that utilises digital cards, PINs, or biometrics. Procedural access control should be based on the establishment of control points with security personnel located in convenient locations, such as at the approach to the outer perimeter or the entrance to the entity's facility. Access control should be implemented for all premises of the entity through direct inspection of security passes by security personnel or by another method of unambiguous identification of a person (such as an automatic access control system), with an appropriate method for maintaining access records. Unauthorised access detection should be carried out to enable an effective and timely response to attempted unauthorised access within the outer perimeter or within the entity's facilities, as well as for subsequent analysis to identify the perpetrators of such actions. Detection of unauthorised access should be carried out in different ways, depending on the established level of physical security of a particular space. Detection of unauthorised

access should be carried out by security personnel, external intervention teams, various electronic systems, or a combination of these measures.

5. Adequately protect the storage of critical data of the entity, which includes data in physical and electronic form, taking into account that the storage of data related to the provision of services from the digital infrastructure sector under Annex I to the Act generally includes data in electronic form. The physical protection of critical data in physical form should be carried out by using appropriate security containers located on premises with an adequate level of physical security measures or by using an open storage area for critical data, without security containers but with an adequate level of physical security measures in place for such premises. The physical protection of critical data in electronic form should be carried out through the physical protection of the premises in which the network and information systems used by entities from the digital infrastructure sector, as under Annex I to the Act, are located, and in particular, where sensitive client computer equipment is located. An entity shall establish rules for the access of persons to all premises where critical data are stored, rules for the introduction of technical equipment, as well as rules for the introduction and use of private technical equipment by employees in premises with different physical security requirements.

6. Premises containing servers and other equipment for the management of the entity's network and information systems shall be organised as specially monitored premises, to which only persons responsible for the security and administration of such systems, i.e. maintenance staff, shall have the right of access, but only when accompanied at all times by persons responsible for the security of the entity and the administration of such systems. An effective access control system and systems for detecting unauthorised access shall be implemented to protect access to such premises. Client computer equipment that is vulnerable to unauthorised physical access shall be located in premises that have an appropriate level of physical security measures and shall be used in such premises, i.e. under the control of a competent employee of the entity. For persons responsible for the management of the measures, as well as persons responsible for the security and administration of the entity's network and information systems, the entity shall obtain data confirming the absence of any criminal record of those persons, i.e. an appropriate certificate of no criminal record, and update the data in question periodically, at least every five years.

ANNEX IV

STATEMENT OF COMPLIANCE OF ESTABLISHED CYBER-SECURITY RISK-MANAGEMENT MEASURES

INFORMATION ABOUT THE ENTITY	
NAME	
ADDRESS	
SECTOR SUBSECTOR TYPE OF ENTITY	
SECTOR MAIN BUSINESS ACTIVITY	

CYBERSECURITY SELF-ASSESSMENT	
IDENTIFIED LEVEL OF CYBERSECURITY RISKS	
LEVEL OF CYBERSECURITY RISK-MANAGEMENT MEASURES DETERMINED AS BINDING	
TOTAL POINTS OF THE DEGREE OF COMPLIANCE OF CYBERSECURITY RISK-MANAGEMENT MEASURES	
TOTAL POINTS OF THE TREND OF RAISING THE MATURITY LEVEL	
LIST OF DOCUMENTS	
NAME, SURNAME AND SIGNATURE OF THE PERSON WHO CONDUCTED THE SELF-ASSESSMENT PROCEDURE	

STATEMENT OF COMPLIANCE	
The results of the cybersecurity self-assessment for the entity indicate that the cybersecurity risk-management measures in place comply with the cybersecurity risk-management measures prescribed by the Cybersecurity Act and the Regulation on Cybersecurity.	
NAME, SURNAME AND SIGNATURE OF THE PERSON RESPONSIBLE FOR MANAGING CYBERSECURITY RISK-MANAGEMENT MEASURES	