VI.

Theses of the implementing legislation for the proposed legislation

It is proposed to issue six by-law implementing regulations – decrees – to the draft law on cyber security. The draft law authorizes the National Office for Cyber and Information Security to issue them. These decrees are:

The Regulation on Regulated Services regulates the criteria for the identification of regulated services, the determination of regimes of providers of regulated services, if their regulated service has been identified according to the Regulation, as well as specific criteria for the identification of strategically important services.

The Decree on the security measures of the regulated service provider in the regime of higher obligations defines both the content and scope of security measures (which are divided into organizational and technical), but also the localization of information and data when they are processed abroad.

The decree on the security measures of the regulated service provider in the regime of lower obligations, which contains the content and scope of security measures, while, unlike the previous decree, it does not contain the localization of information and data, but on the contrary includes the method of determining the significance of the impact of a cyber security incident .

The Decree on the NÚKIB Portal contains, in particular, the types and methods of reporting data from regulated service providers and cyber security incidents.

The Decree on Indispensable Functions of a Specified Scope sets out the critical functions of the scope of assets that are subject to cyber security management under the Act.

The decree on supplier risk criteria follows on from the supplier assessment mechanism and specifies the supplier risk criteria and the method of their evaluation.

Decree on Regulated Services

Proposal

DECREE

from dd.mm.yyyy ,

on regulated services

The National Office for Cyber and Information Security establishes pursuant to § 55 paragraph 1 letter a), b) and f) of Act No. [to be added], on cyber security (hereinafter referred to as "the Act"):

§ 1

Subject of legislation

This decree incorporates the relevant regulation of the European Union [1]and regulates

a) criteria for identifying regulated services (§ 4 of the Act),
b) determining the regimes of the regulated service provider in connection with the identified regulated services (Section 6(3) of the Act) and
c) criteria for identifying a strategically important service (Section 27, paragraph 1 of the Act).

§ 2

Definition of terms

(1) For the purposes of this decree, it is understood

a) micro-enterprise means a micro-enterprise according to Commission Recommendation 2003/361/EC of 6 May 2003 on the definition of micro-enterprises and small and medium-sized enterprises,
b) small business means a small business according to Commission Recommendation 2003/361/EC of 6 May 2003 on the definition of micro and small and medium-sized enterprises,
c) medium-sized enterprise means a medium-sized enterprise according to Commission Recommendation 2003/361/EC of 6 May 2003 on the definition of micro-enterprises and small and medium-sized enterprises,
d) a large enterprise is an enterprise exceeding the values for a medium-sized enterprise according to Commission Recommendation 2003/361/EC of May 6, 2003 on the definition of micro-enterprises and small and medium-sized enterprises ,
e) by the CZ-NACE classification of economic activities according to the announcement of the Czech Statistical Office No. 244/2007 Coll., on the introduction of the Classification of Economic Activities,
f) sensitive research activity activity aimed at research and development of sensitive dual-

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive) .

use goods and sensitive dual-use technologies within the meaning of Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 establishing a Union regime for export control, mediation, technical aid, transit and transport of dual-use goods.

(2) When calculating the size of the company, it is also necessary to consider the relevant ties between related organizations.

(3) For the purposes of this decree, the amounts stated in the euro currency are converted to the Czech currency according to the average exchange rate announced by the Czech National Bank for the previous calendar year.

(4) Deviating from the rules of Commission Recommendation 2003/361/EC of 6 May 2003 on the definition of micro-enterprises and small and medium-sized enterprises for the purposes of this decree, if the founder or founder of the assessed organization is a territorial self-governing unit, this territorial self-governing unit is not taken into account when determining the size of the undertaking, if that provider of the regulated service is independent in terms of the network and information systems it uses in the provision of its services and in terms of the services it provides.

§ 3

Regulated services

A regulated service defined as a criterion for identifying a regulated service according to Section 4 of the Act is a service which

a) is listed in the annex to this decree and
b) it is performed by an authority or a person meeting the criterion of a regulated service provider listed in the annex to this decree.

§ 4

Regulated service provider regime corresponding to a specific regulated service

(1) The annex to this decree establishes the regime of the regulated service provider for each regulated service.

(2) In the event that the provider of a regulated service fulfills the criteria of a provider of a regulated service corresponding to the regime of higher and lower obligations at the same time in connection with one regulated service, the regime of the provider of the regulated service for this regulated service is the regime of higher obligations.

§ 5

Criteria for identifying a strategically important service

A strategically important service determined on the basis of the criteria for identifying a strategically important service is a service listed in the Annex to this Decree, if it is performed by an authority or person meeting the criteria of a regulated service provider listed in the Annex to this Decree in

a) Sector 1. Public administration, service 1.1. Exercise of delegated powers, point I. letter a) to i),
b) Sector 2. Energy - Electricity , service 2.1. Electricity production, point I. letter b),

c) Sector 2. Energy - Electricity , service 2.2. Operation of the electricity transmission system,
d) Sector 2. Energy - Electricity , service 2.3. Operation of the electricity distribution system, point I. letter b) ,
e) Sector 3. Energy - Oil and oil products, service 3.4. Oil pipeline operation, point I.,
f) Sector 3. Energy - Oil and oil products, service 3.5. Operation of the product line, point I.,
g) Sector 4. Energy - Gas industry , service 4.2. Operation of the gas transmission system ,
h) Sector 4. Energy - Gas industry , service 4.3. Operation of the gas distribution system, point I.,
i) Sector 12. Air transport, service 12.4. Air traffic control over the airspace of the Czech Republic,
j) Sector 12. Air transport, service 12.9. Flight navigation services, point I.,
k) Branch 13. Rail transport, service 13.1. Construction of train routes on a national level,
l) Sector 16. Digital infrastructure and services, service 16.1. Provision of a publicly available electronic communications service , point I. letter c) and d),
m) Sector 16. Digital infrastructure and services, service 16.2. Ensuring the public communication network of electronic communications, point I. letter c) and d),
n) Sector 16. Digital infrastructure and services, service 16.5. Administration and operation of the registry of Internet top-level domains, or
o) Sector 16. Digital infrastructure and services, service 16.6. Provision of cloud computing services , point I. letter b).

§ 6

Effectiveness

This decree becomes effective on dd.mm.yyyy .

Director:
Ing. Lukáš Kintr incl

Annex to Decree No. [to be added] Coll.
Criteria for identifying a regulated service

1. Public administration

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
1.1. Exercise of delegated powers	The body or person is I. provider of a regulated service in the regime of higher obligations, if it is a) by the central state administration body, b) an administrative office with nationwide jurisdiction, including the headquarters and general directorate of territorially decentralized (specialized) state administration bodies, c) Office of the President of the Republic, d) Senate Office, e) Office of the Chamber of Deputies, f) the Czech National Bank, g) Police Presidium, h) a police unit with nationwide jurisdiction, i) General Directorate of the Fire and Rescue Service, j) the regional directorate of the fire brigade, k) Office of the Public Defender of Rights, l) by the Supreme Audit Office, m) judicial authority, n) the public prosecutor's office, o) health insurance company, p) by region, q) the capital Prague, or r) municipalities with extended jurisdiction with at least 125,000 inhabitants, II. regulated service provider under the reduced duty regime, if any a) territorially deconcentrated (specialized) state administration body, b) professional chamber, c) a university, d) Academy of Sciences of the Czech Republic, or e) municipalities with extended jurisdiction with a population of up to 125,000.

2. Energy - Electricity

Regulated service

Service	Regulated service provider criteria and its regime for that service
2.1. Electricity production	The holder of a license to produce electricity according to the Energy Act is I. provider of a regulated service in the regime of higher obligations, in the event that a) is a large enterprise, or b) has a production plant with a total installed electrical output of at least 100 MW, II. provider of a regulated service in the regime of lower

	obligations, in the event that a) is a medium-sized enterprise, or b) has a production facility with a total installed electrical output of at least 50 MW, but less than 100 MW.
2.2. Operation of the electricity transmission system	The holder of a license for the transmission of electricity according to the Energy Act is a regulated service provider under the regime of higher obligations.
2.3. Operation of the electricity distribution system	The holder of the electricity distribution license under the Energy Act is I. provider of a regulated service in the regime of higher obligations, in the event that a) is a large enterprise, or b) its transmission capacity of the distribution system is at least 220 MW, II. provider of a regulated service in the regime of lower obligations, in the event that a) is a medium-sized enterprise, or b) its transmission capacity of the distribution system is at least 120 MW, but less than 220 MW.
2.4. Electricity trade	The holder of a license to trade in electricity according to the Energy Act is I. provider of a regulated service in the regime of higher obligations, in the event that a) is a large enterprise, or b) the number of its collection and delivery points is an average of 50,000 for the last available calendar year, II. provider of a regulated service in the regime of lower obligations, in the event that a) is a medium-sized enterprise, or b) the number of its collection and delivery points is an average of 10,000, but less than 50,000, for the last available calendar year.
2.5. Performance of the activity of the nominated organizer of the electricity market	The holder of a license for the activities of a market operator according to the Energy Act is a regulated service provider under the regime of higher obligations.
2.6. Carrying out the activity of electricity sales or generation, aggregation or demand-side response or energy storage, including issuing orders to trade in one or more electricity markets, including regulatory energy markets	An electricity market participant that buys, sells or produces electricity, performs aggregation services or is a demand-side response operator or an energy storage operator, including issuing trading orders, in one or more electricity markets, including regulation energy markets is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.

2.7. Operation of charging stations	The operator of a publicly accessible charging station according to the Act on Fuels, who is responsible for the management and operation of a charging station that provides a charging service to end users on behalf of and on behalf of the mobility provider is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.

3. Energy - Petroleum and petroleum products

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
3.1. Oil extraction	The operator of the oil extraction facility is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
3.2. Oil processing	The operator of the oil processing facility is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
3.3. Operation of storage equipment	The operator of a storage facility for the storage of oil or oil products is I. provider of a regulated service in the regime of higher obligations, in the event that a) is a large enterprise, or b) has a reservoir or a complex of reservoirs with a total capacity of at least 40,000 m^3, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
3.4. Oil pipeline operation	The operator of the oil pipeline is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
3.5. Product pipeline operation	The operator of the pipeline is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
3.6. Performance of the	The Central Stockpile Administrator under the Emergency

activity of the central inventory manager	Petroleum Stockpile Act is a regulated service provider under the enhanced duty regime.
3.7. Fuel filling station operation	A gas station operator is a regulated service provider under the regime of higher obligations, if it operates 100 or more gas stations in the territory of the Czech Republic.

4. Energy - Gas industry

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
4.1. Gas production	The holder of a gas production license under the Energy Act is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
4.2. Operation of the gas transportation system	The holder of a license for the transport of gas according to the Energy Act is a regulated service provider under the regime of higher obligations.
4.3. Operation of the gas distribution system	The holder of a gas distribution license under the Energy Act is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
4.4. Gas store	The holder of a license for gas trade under the Energy Act is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
4.5. Gas storage	The holder of a gas storage license under the Energy Act is I. provider of a regulated service in the regime of higher obligations, in the event that a) is a large enterprise, or b) operates an underground gas storage facility with a projected installed capacity of at least 200 million ^{m3} II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.

5. Energy - Heating industry

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
5.1. Thermal energy	The holder of a license for the production of thermal energy

production	according to the Energy Act is I. provider of a regulated service in the regime of higher obligations, in the event that a) is a large enterprise, or b) has a thermal energy source with a total installed thermal output of at least 200 MW, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
5.2. Operation of the thermal energy supply system	The holder of a license for the distribution of thermal energy according to the Energy Act is I. provider of a regulated service in the regime of higher obligations, in the event that a) is a large enterprise, or b) has a thermal energy supply system with a total transmission capacity of at least 160 MW, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.

6. Energy - Hydrogen

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
6.1. Hydrogen production	The hydrogen producer is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
6.2. Hydrogen storage	The entity providing hydrogen storage is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
6.3. Hydrogen transport	The entity providing hydrogen transport is I. provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.

7. Manufacturing industry

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
7.1. Production of	A manufacturer of computers, electronic and optical devices

computers, electronic and optical devices and equipment	and equipment within the meaning of section 26 of the CZ-NACE classification, which is a large or medium-sized enterprise, is a regulated service provider under the regime of lower obligations.
7.2. Production of electrical equipment	A manufacturer of electrical equipment within the meaning of section 27 of the CZ-NACE classification, which is a large or medium-sized enterprise, is a regulated service provider under the regime of lower obligations.
7.3. Manufacture of machinery and equipment not classified under other sections of the CZ-NACE classification	A manufacturer of machinery and equipment not classified elsewhere within the meaning of section 28 of the CZ-NACE classification, which is a large or medium-sized enterprise, is a regulated service provider under the regime of lower obligations.
7.4. Manufacture of motor vehicles (except motorcycles), trailers and semi-trailers	The manufacturer of motor vehicles, trailers and semi-trailers in the sense of section 29 of the CZ-NACE classification is I. a regulated service provider in the regime of higher obligations in the event that it serially produces passenger motor vehicles, II. a regulated service provider under the regime of lower obligations, if it is a large or medium-sized enterprise.
7.5. Production of other means of transport and equipment	A manufacturer of other means of transport and equipment within the meaning of section 30 of the CZ-NACE classification, which is a large or medium-sized enterprise, is a regulated service provider under the regime of lower obligations.

19. Science, research and education

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
19.1. Research and Development	A research organization whose main objective is to carry out applied research or experimental development with a view to exploiting this research for commercial purposes, a university or other research organization [31]is a regulated service provider under the higher obligations regime if a) performs sensitive research activity, or b) most of the conducted research projects are financed by more than 50% from public sources. A research organization whose main objective is to carry out applied research or experimental development with a view to

[31] List of research organizations maintained in accordance with § 33a of Act No. 130/2002 Coll., on the support of research and development from public funds and on the amendment of some related laws (Act on the Support of Research and Development)

	exploiting that research for commercial purposes, or a higher education institution is a regulated service provider under the reduced duty regime if it is a medium-sized or large enterprise.
19.2. Operation of a large research infrastructure	Host or partner institution of a large research infrastructure[32] or the European research infrastructure consortium is a provider of a regulated service under the regime of higher obligations.

20. Postal and courier services

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
20.1. Providing postal and courier services	A postal service operator under the Postal Services Act and a courier service provider under a directly applicable European Union regulation [33]that provides at least one of the steps in the postal chain that is a medium-sized or large enterprise is a regulated service provider in the lower duty regime.

21. Military industry

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
21.1. Production of military equipment	The manufacturer of military equipment listed in the list of military equipment according to the Act on Foreign Trade in Military Equipment is I) provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II) a regulated service provider in the regime of lower obligations if it is a medium-sized enterprise.
21.2. Military equipment store	A legal or natural person that has been issued a permit for trade in military material pursuant to the Act on Foreign Trade in Military Material is I) provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II) a regulated service provider in the regime of lower obligations if it is a medium-sized enterprise.
21.3. Production of dual-use goods and technologies	The manufacturer of dual-use goods according to the directly applicable regulation of the European Union [34]is I) provider of a regulated service under the regime of higher

[32] § 2 paragraph 2 letter d) Act No. 130/2002 Coll., on the support of research and development from public funds and on the amendment of some related laws (Act on the Support of Research and Development)

[33] Regulation (EU) 2018/644 of the European Parliament and of the Council of 18 April 2018 on cross-border parcel delivery services

	obligations, if it is a large enterprise, II) a regulated service provider in the regime of lower obligations if it is a medium-sized enterprise.
21.4. Export of dual-use goods and technologies	The holder of a permit for the export of dual-use goods and technologies according to the directly applicable regulation of the European Union [35]is I) provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II) a regulated service provider in the regime of lower obligations if it is a medium-sized enterprise.
21.5. Intermediation of dual-use goods and technologies	The holder of a permit for the provision of intermediary services for dual-use goods and technologies according to the directly applicable regulation of the European Union [36]is I) provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II) a regulated service provider in the regime of lower obligations if it is a medium-sized enterprise.
21.6. Technical assistance for dual-use goods and technologies	The holder of an authorization for the provision of technical assistance related to dual-use goods and technology under a directly applicable regulation of the European Union [37]is I) provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II) a regulated service provider in the regime of lower obligations if it is a medium-sized enterprise.
21.7. Transit and transport of dual-use goods and technologies	The holder of a permit for the transit or transport of dual-use goods and technologies according to the directly applicable regulation of the European Union [38]is I) provider of a regulated service under the regime of higher obligations, if it is a large enterprise, II) a regulated service provider in the regime of lower obligations if it is a medium-sized enterprise.

22. The space industry

Regulated service	
Service	**Regulated service provider criteria and its regime for that service**
22.1. Ensuring support for the provision of services using outer space	A ground infrastructure operator who is a medium-sized or large enterprise and at the same time does not provide this support service as an entrepreneur providing an electronic

[35] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 establishing a Union regime for the control of exports, brokering, technical assistance, transit and transport of dual-use items (recast)

[36] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 establishing a Union regime for the control of exports, brokering, technical assistance, transit and transport of dual-use items (recast)

8. Food industry

Service	Regulated service Regulated service provider criteria and its regime for that service
8.1. Food production	According to the directly applicable regulation of the European Union, a food business [2] that deals with wholesale distribution and industrial production and processing of food is a regulated service provider in the regime of lower obligations, if it is a large enterprise or a medium-sized enterprise.
8.2. Food processing	According to the directly applicable regulation of the European Union, a food business [3] that deals with wholesale distribution and industrial production and processing of food is a regulated service provider in the regime of lower obligations, if it is a large enterprise or a medium-sized enterprise.
8.3. Food distribution	According to the directly applicable regulation of the European Union, a food business [4] that deals with wholesale distribution and industrial production and processing of food is a regulated service provider in the regime of lower obligations, if it is a large enterprise or a medium-sized enterprise.

9. Chemical industry

Service	Regulated service Regulated service provider criteria and its regime for that service
9.1. Manufacture of hazardous chemical substances, mixtures or preparations or substances	The manufacturer of dangerous chemical substances, mixtures or preparations or substances according to the directly applicable regulation of the European Union [5] is I. a regulated service provider in the regime of higher obligations if he is the operator or user of an object classified

9.4. Production of items listed in Article 3 point 3 of the directly applicable regulation of the European Union [8] from substances or mixtures	The manufacturer of articles according to the directly applicable regulation of the European Union [9] from substances or mixtures is I. a regulated service provider in the regime of higher obligations if he is the operator or user of an object classified in group B according to the Act on the Prevention of Serious Accidents, II. a provider of a regulated service under the reduced duty regime in the event that a) is a large enterprise, b) is a medium-sized enterprise, or c) is the operator or user of an object classified in group A according to the Act on Prevention of Serious Accidents.

10. Water management

Service	Regulated service Regulated service provider criteria and its regime for that service
10.1. Water supply operation	The water supply operator according to the Water Supply and Sewerage Act is I. provider of a regulated service in the regime of higher obligations, in the event that a) is a large enterprise, or b) supplies drinking water to at least 50,000 inhabitants, II. a regulated service provider in the regime of lower obligations, if it is a medium-sized enterprise.
10.2. Sewage operation	The sewerage operator according to the Act on Waterworks and Sewage is I. provider of a regulated service in the regime of higher obligations, in the event that a) is a large enterprise, or b) provides waste water removal or treatment services to at least 50,000 inhabitants, II. a regulated service provider in the regime of lower

[2] Article 3 Point 2 Regulation (EC) No. 178/2002 of the European Parliament and of the Council of 28 January 2002 establishing the general principles and requirements of food law, establishing the European Food Safety Authority and establishing procedures relating to food safety

[3] Article 3 Point 2 Regulation (EC) No. 178/2002 of the European Parliament and of the Council of 28 January 2002 establishing the general principles and requirements of food law, establishing the European Food Safety Authority and establishing procedures relating to food safety

[4] Article 3 Point 2 Regulation (EC) No. 178/2002 of the European Parliament and of the Council of 28 January 2002 establishing the general principles and requirements of food law, establishing the European Food Safety Authority and establishing procedures relating to food safety

[5] Regulation (EC) No. 1907/2006 of the European Parliament and of the Council of 18 December 2006 on the registration, evaluation, authorization and restriction of chemical substances, on the establishment of the European Chemicals Agency, on the amendment of Directive 1999/45/EC and on the repeal of the Council Regulation (EEC) No. 793/93, Commission Regulation (EC) No. 1488/94, Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/ 21/EC

[6]Regulation (EC) No. 1907/2006 of the European Parliament and of the Council of 18 December 2006 on the registration, evaluation, authorization and restriction of chemical substances, on the establishment of the European Chemicals Agency, on the amendment of Directive 1999/45/EC and on the repeal of the Council Regulation (EEC) No. 793/93, Commission Regulation (EC) No. 1488/94, Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/ 21/EC

[7]Regulation (EC) No. 1907/2006 of the European Parliament and of the Council of 18 December 2006 on the registration, evaluation, authorization and restriction of chemical substances, on the establishment of the European Chemicals Agency, on the amendment of Directive 1999/45/EC and on the repeal of the Council Regulation (EEC) No. 793/93, Commission Regulation (EC) No. 1488/94, Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/ 21/EC

[8]Regulation (EC) No. 1907/2006 of the European Parliament and of the Council of 18 December 2006 on the registration, evaluation, authorization and restriction of chemical substances, on the establishment of the European Chemicals Agency, on the amendment of Directive 1999/45/EC and on the repeal of the Council Regulation (EEC) No. 793/93, Commission Regulation (EC) No. 1488/94, Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/ 21/EC

[9]Regulation (EC) No. 1907/2006 of the European Parliament and of the Council of 18 December 2006 on the registration, evaluation, authorization and restriction of chemical substances, on the establishment of the European Chemicals Agency, on the amendment of Directive 1999/45/EC and on the repeal of the Council Regulation (EEC) No. 793/93, Commission Regulation (EC) No. 1488/94, Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/ 21/EC

10Regulation (EC) No. 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules for the protection of civil aviation against illegal acts

11 Regulation (EC) No. 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules for the protection of civil aviation against illegal acts

Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges

[12]Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 establishing a framework for the creation of a single European sky

13 Regulation (EC) No. 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules for the protection of civil aviation against illegal acts

14 Regulation (EC) No. 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules for the protection of civil aviation against illegal acts

15 Regulation (EC) No. 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules for the protection of civil aviation against illegal acts .

[16]Regulation (EC) No. 549/2004 of the European Parliament and of the Council of 10 March 2004 establishing a framework for the creation of a single European sky.

[17]Article 7 and Article 9 of Regulation No. 550/2004 of the European Parliament and of the Council of March 10, 2004, on the provision of flight navigation services in the single European sky.

[18] Regulation (EC) No. 725/2004 of the European Parliament and of the Council of 31 March 2004 on improving the security of ships and port facilities

[19] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security

[20] Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community control and information system for the operation of vessels and repealing Council Directive 93/75/EEC

[21]§ 6i of Act No. 365/2000 Coll., on public administration information systems and on the amendment of certain laws, as amended on February 1, 2022.

[22] Regulation (EU) No. 575/2013 of the European Parliament and Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No. 648/2012

[23] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC

Decree on the security measures of the regulated service provider in the regime of higher obligations

Proposal

DECREE

from dd.mm.yyyy ,

on the security measures of the provider of the regulated service in the regime of higher obligations

The National Office for Cyber and Information Security establishes pursuant to § 55 paragraph 1 letter c) Act No. [to be added] Coll., on cyber security (hereinafter referred to as "the Act"):

PART ONE

INTRODUCTORY PROVISIONS

§ 1

Subject of legislation

This decree incorporates the relevant regulation of the European Union [39]and for regulated service providers in the regime of higher obligations (hereinafter referred to as the "obligated person") regulates

a) content and scope of security measures a
b) information and data to which the obligee's obligation to ensure their processing in a defined territory and these defined territories applies.

derivatives, central counterparties and trade repositories

[24] § 7 of Act No. 370/2017 Coll., on payment systems

[25]§ 66 of Act No. 370/2017 Coll., on payment systems

[26] Art. 15 EU Regulation of 23 November 2022 on serious cross-border health threats and on the repeal of Decision No. 1082/2013/EU

[27]Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical evaluations of medicinal products for human use and repealing Directive 2001/20/EC

[28] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No. 178/2002 and Regulation (EC) No. 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

[29]Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU

[30] Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on the enhanced role of the European Medicines Agency in crisis preparedness and crisis management in the field of medicinal products and medical devices

[38] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 establishing a Union regime for the control of exports, brokering, technical assistance, transit and transport of dual-use items (recast)

[37] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 establishing a Union regime for the control of exports, brokering, technical assistance, transit and transport of dual-use items (recast)

§ 2

Definition of terms

For the purposes of this decree, it is understood

a) administrator, a privileged user or a person ensuring the management, operation, use, maintenance and security of a technical asset,

b) acceptable risk is a risk that is acceptable to the obligated person,

c) a security policy is a set of principles and rules that determine the way to ensure the protection of assets,

d) risk assessment the overall process of identification, analysis and evaluation of risks,

e) a privileged user is a user or person whose activity on a technical asset may have a significant impact on the security of the regulated service,

f) risk is the possibility that a certain threat will exploit an asset's vulnerability and cause damage,

g) risk management a systematic process including risk assessment, implementation of security measures to manage risks and risk communication,

h) by the information security management system, part of the management system of the obliged entity based on the approach to the risks of assets, which determines the method of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the security of information and data,

i) the user is a natural or legal person or public authority that uses the assets,

j) top management means the person or group of persons who manage the obliged entity, or the statutory body of the obligated entity, and

k) a significant change is a change that has or may affect cyber security and is determined based on established rules, procedures and criteria.

PART TWO

SAFETY PRECAUTIONS

§ 3

The obligated person shall introduce and implement security measures in accordance with this legal regulation within the scope of cyber security management established pursuant to Section 13 of the Act (hereinafter referred to as the "specified scope").

TITLE I

ORGANIZATIONAL MEASURES

§ 4

Information security management system

(1) Mandatory person within the information security management system

a) establishes the objectives of the information security management system aimed at ensuring the security of the regulated service,
b) based on the objectives of the information security management system, security needs and risk assessment, it will implement adequate security measures aimed at ensuring the security of the regulated service,
c) manages risks according to § 9,
d) create and approve a security policy in relation to the management of cyber security, which contains the main principles, objectives of the information security management system, security needs, rights and obligations in relation to the management of information security, and based on the security needs and the results of the risk assessment, determine the security policy and security documentation in other areas according to § 7,
e) ensure the execution of a cyber security audit according to § 17,
f) shall ensure an evaluation of the effectiveness of the information security management system it contains at least once a year
    1. evaluation of the objectives of the information security management system aimed at ensuring the security of the regulated service,
    2. assessment of the fulfillment of the risk management plan prepared in accordance with § 9 letter G),
    3. assessment of the state of the information security management system, including revision of the risk assessment,
    4. assessment of the results of cyber security audits and controls in the field of cyber security,
    5. the results of previous evaluations of the effectiveness of the information security management system carried out in accordance with this letter,
    6. assessment of the impact of cyber security incidents on the services provided pursuant to § 16 and on the area of cyber security a
    7. assessment of significant changes according to § 12,
g) based on the evaluation of the effectiveness of the information security management system according to letter f) prepares a report on the review of the information security management system,
h) continuously identifies and subsequently manages significant changes in accordance with § 12,
i) updates the information security management system and relevant documentation based on
    1. findings of cyber security audits and controls in the field of cyber security,
    2. the results of the evaluation of the effectiveness of the information security management system,
    3. the effects of cyber security incidents on the services provided and
    4. in connection with the significant changes being made,
j) manages the operation and resources of the information security management system and records activities related to the information security management system and risk management and
k) establishes the process of managing exceptions to the rules established under letter d).

(2) Obliged person in the event of non-fulfillment of the risk management obligation pursuant to paragraph 1 letter C)

a) implements all security measures required by this decree,
b) elaborates on security measures according to letter and),
   1. declaration of applicability according to § 9 paragraph 1 letter f) a
   2. risk management plan adequately according to § 9 paragraph 1 letter G),
c) will take into account in the risk management plan
   1. significant changes,
   2. changes of the specified scope according to Section X of the Act,
   3. countermeasures according to Section X of the Act,
   4. cyber security incidents, including those previously addressed,
   5. results of cyber security audits and cyber security controls a
   6. results of penetration testing and vulnerability scanning,
d) implements security measures in accordance with the risk management plan.

§ 5

Duties of top management

(1) Senior management with regard to the information security management system

a) demonstrably participates in training according to § 11 paragraph 3 letter and),
b) ensure the determination of the security policy and objectives of the information security management system according to § 4, compatible with the strategic orientation of the obliged entity,
c) will ensure the integration of the information security management system into the processes of the obliged entity,
d) ensure the availability of resources needed for the information security management system,
e) informs employees about the importance of the information security management system and the importance of achieving compliance with its requirements with all concerned parties,
f) will ensure support for achieving the objectives of the information security management system,
g) leads employees to develop the effectiveness of the information security management system and supports them in this development,
h) participates in the development of the impact analysis according to § 16,
i) promotes continuous improvement of the information security management system,
j) supports those in security roles in promoting cyber security in their areas of responsibility,
k) ensure the establishment of rules for determining administrators and persons who will hold security roles,
l) ensure that confidentiality is maintained for all relevant persons (e.g. administrators, persons holding security roles, persons with access to sensitive information, suppliers, etc.)
m) ensure appropriate authority and resources, including budgetary resources, for

persons holding security roles to fulfill their roles and perform related tasks; and

n) ensure the testing of business continuity plans, recovery plans and processes associated with managing cyber security incidents.

(2) Top management is demonstrably getting to know each other

a) the report on the review of the information security management system,
b) a risk assessment report,
c) the results of the impact analysis in accordance with § 16 a
d) results of cyber security audits and cyber security controls.

(3) Senior management within the information security management system will determine the composition of the cyber security management committee, security roles, their rights and responsibilities related to the information security management system.

(4) The meetings of the Cyber Security Management Committee take place at regular intervals and a documented record is kept of their progress.

(5) The cyber security management committee is made up of persons with the relevant powers and expertise for the overall management and development of the information security management system and persons significantly involved in the management and coordination of activities related to cyber security, whose member must be at least one representative of the top management or one authorized by him cyber security person and manager. The responsible person at the cyber security management committee will take into account the recommendations listed in Appendix No. 6 to this decree.

(6) Senior management will designate a person to fill the security role

a) cyber security manager,
b) cyber security architect,
c) asset guarantor a
d) cyber security auditor.

(7) Top management will ensure the replaceability of the security roles listed in paragraph 6 letter a) and b).

§ 6

Security role

(1) Cyber Security Manager

a) is a security role responsible for the information security management system, while the performance of this role can be entrusted to a person who is trained for this activity and demonstrates professional competence through experience with cyber security management or information security management
   1. for a period of at least three years, or
   2. for a period of one year if she completed her studies at university,
b) is responsible for regularly informing top management about
   1. activities resulting from the scope of his responsibility and
   2. the state of the information security management system,
c) may not be entrusted with roles responsible for the operation of a regulated service.

(2) Cyber Security Architect is a security role responsible for ensuring the design of the implementation of security measures to ensure the secure architecture of the regulated

service, and this role may be assigned to a person who is trained for this activity and demonstrates professional competence through practice in designing the implementation of security measures and ensuring security architecture

a) for a period of at least three years, or
b) for one year if she completed her studies at a university.

(3) An asset guarantor is a security role responsible for ensuring the development, use and security of an asset.

(4) Cyber Security Auditor

a) is a security role responsible for conducting a cyber security audit, and this role may be assigned to a person who is trained for this activity and demonstrates professional competence through practice in conducting cyber security audits or information security management system audits
   1. for a period of at least three years, or
   2. for a period of one year if she completed her studies at university,
b) guarantees that the conduct of the cyber security audit is impartial and
c) may not be assigned to perform other security roles.

(5) When determining persons holding security roles, the obliged person shall take into account the recommendations listed in Annex No. 6 to this decree.

§ 7

Security policy management and security documentation

(1) Mandatory person in the management of security policy and security documentation

a) establishes a security policy and maintains security documentation covering the areas listed in Annex No. 5 to this decree and
b) in the operating documentation, it establishes rules and procedures that take into account the relevant areas from the safety policy and safety documentation.

(2) The obliged person shall comply with the rules and procedures established pursuant to paragraph 1.

(3) The obliged person regularly reviews the safety policy and safety documentation, ensures that they are up-to-date and that their relevant areas are taken into account in the operational documentation.

(4) The obliged person shall designate the person responsible for the regular review and updating of the safety policy, safety documentation and consideration of their relevant areas in the operational documentation pursuant to paragraph 3.

(5) Security policy and security documentation must be managed to be

a) available in electronic or paper form,
b) communicated within the bound person,
c) reasonably available to the parties concerned,
d) protected from the point of view of confidentiality, integrity and availability and
e) conducted so that the information contained in them is complete, legible, correct, easily identifiable and searchable.

§ 8

Asset management

Obliged person in accordance with the identification and registration of assets

a) establishes a methodology for the identification and evaluation of assets, including the determination of asset levels at least to the extent specified in Annex No. 1 to this decree,

b) determine and register asset guarantors,

c) evaluates primary assets from the point of view of confidentiality, integrity and availability and assigns them to individual levels according to letter and),

d) as part of the assessment of primary assets, it assesses at least the areas listed in Annex No. 1 to this decree,

e) identifies and records relevant links between assets,

f) assesses supporting assets and takes into account in particular links to primary assets and

g) for individual levels of assets according to letter a) establishes and implements protection rules necessary to ensure their confidentiality, integrity and availability, which include in particular

   i) permissible ways of using assets,

   ii) asset handling rules,

   iii) rules for classification of information,

   iv) asset tagging rules,

   v) exchangeable media management rules,

   vi) rules for secure electronic sharing and physical transfer of assets a

   vii) rules for determining the method of disposal of information and data and their copies and disposal of technical assets that are carriers of information and data with regard to the level of assets in accordance with Annex No. 4 to this decree.

§ 9

Risk management

(1) Mandatory person in the framework of risk management following § 8

a) establishes a methodology for the identification and assessment of risks, including the establishment of criteria for the acceptability of risks,

b) when identifying risks with respect to assets, identifies relevant threats and vulnerabilities; in doing so, it considers in particular the categories of threats and vulnerabilities listed in Annex No. 3 to this decree,

c) conducts risk assessments at regular intervals at least once a year and in case of significant changes,

[34] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 establishing a Union regime for the control of exports, brokering, technical assistance, transit and transport of dual-use items (recast)

[39] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive) .

d) when assessing risks, take into account relevant threats and vulnerabilities according to letter b) and assess possible impacts on assets, based on the assessment of assets according to § 8; assesses these risks at least to the extent of Annex No. 2 to this decree,

e) on the basis of the performed risk assessment according to letter d) prepares a risk assessment report,

f) based on the security needs and the results of the risk assessment, prepares a statement of applicability, which contains an overview of all the security measures required by this decree, which

1. was not applied, including justification and an overview of the alternative security measures taken,
2. was applied, including the method of fulfillment,

g) on the basis of the risk assessment carried out in accordance with letter d) prepares a risk management plan, which it contains

1. description of security measures,
2. goals and benefits of security measures for managing individual risks,
3. designation of the person ensuring the introduction of security measures for risk management,
4. anticipated human, financial and technical resources for the introduction of security measures,
5. the required date for the introduction of security measures,
6. description of the links between the risks and the relevant security measures a
7. way of implementing security measures,

h) takes into account in the risk assessment and in the risk management plan

1. significant changes,
2. changes of the specified scope according to Section X of the Act,
3. countermeasures according to Section X of the Act,
4. cyber security incidents, including those previously addressed,
5. results of cyber security audits and cyber security controls,
6. results of penetration testing and vulnerability scanning a
7. notification of the risk associated with the supplier according to Section X of the Act.

(2) The obliged person implements security measures in accordance with the risk management plan.

(3) Risk management can also be ensured in other ways than that specified in paragraph 1 letter d) if the obligated person ensures the same or a higher level of risk management process.

§ 10

Management of suppliers

(1) Mandatory person

a) establishes rules for suppliers that take into account the requirements of the information security management system,

b) acquaints its suppliers with the rules according to letter a) and requires

compliance with these rules,

c) identifies and registers its significant suppliers,
d) verifiably informs its important suppliers in writing about their records according to letter c).
e) manages risks associated with suppliers,
f) in connection with the management of risks associated with significant suppliers, ensure that the contracts concluded with significant suppliers contain the relevant areas listed in Annex No. 7 to this decree and
g) regularly reviews the fulfillment of contracts with important suppliers from the point of view of the information security management system.

(2) Mandatory person for important suppliers further
a) within the framework of the tender procedure and before the conclusion of the contract, it assesses the risks related to the fulfillment of the subject of the tender procedure in accordance with Annex No. 2 to this decree,
b) within the framework of concluded contractual relations, it determines the methods and levels of implementation of security measures and determines the content of mutual contractual responsibility for the introduction and control of security measures,
c) conducts regular risk assessments and regular checks of established security measures for services provided using its own resources or with the help of a third party and
d) in response to risks and detected deficiencies, they will ensure their solution.

(3) Requirements for provable information according to paragraph 1 letter d) are
a) identification of the liable person,
b) identification of the regulated service,
c) identification of a significant supplier,
d) notification of the fact that the supplier is a significant supplier for the liable person and
e) content of the rules according to paragraph 1 letter and).

§ 11

Security of human resources

(1) In the context of human resource security management, the responsible person, taking into account the state and needs of the information security management system, establishes a plan for the development of security awareness, the aim of which is to ensure adequate education and improvement of security awareness, including the form, content and scope of instruction and training according to paragraph 2.

(2) The obliged person shall include in the plan the development of security awareness
a) instructing top management on their duties, on security policy, especially in the areas of the information security management system and risk management,
b) instructing users, administrators, persons holding security roles and suppliers about their obligations and the security policy,
c) necessary theoretical and practical training for users, administrators and persons

holding security roles,

d) rules for creating secure passwords in accordance with § 20,

e) relevant topics listed in Annex No. 8 of this decree.

(3) Mandatory person in the framework of human resource security management

a) in accordance with the plan for the development of security awareness, he will ensure the training of top management about his duties, about the security policy, especially in the area of the information security management system and risk management in the form of introductory and regular trainings,

b) in accordance with the security awareness development plan, ensure that users, administrators, persons holding security roles and suppliers are instructed about their obligations and the security policy in the form of introductory and regular trainings,

c) for persons occupying security roles, in accordance with the security awareness development plan, they will provide regular professional training, based on the current needs of the obligated person in the field of cyber security,

d) in accordance with the security awareness development plan, ensure regular training and verification of employees' security awareness in accordance with their job duties,

e) determine the persons responsible for the implementation of the individual activities listed in the security awareness development plan,

f) evaluates the effectiveness of the security awareness development plan, conducted instruction, training and other activities related to improving security awareness,

g) ensure compliance with the security policy by users, administrators and persons holding security roles,

h) determine the rules and procedures for dealing with cases of violations of established security rules by users, administrators and persons holding security roles and

i) in the event of the termination of the contractual relationship with administrators and persons holding security roles, they will ensure the transfer of responsibilities.

(4) The obliged person keeps reports on instruction and training according to paragraph 3, which contain the subject of the instruction and training, including a list of persons who have completed the instruction and training.

§ 12

Management of changes

(1) Mandatory person in the context of asset change management

a) identifies changes that have or may have an impact on cyber security,

b) establishes rules, procedures and criteria for determining significant changes and

c) for changes identified under letter a) determines significant changes in accordance with letter b).

(2) Mandatory person for significant changes

a) documents their management,

b) carries out a risk assessment,
c) takes security measures to reduce all adverse impacts associated with significant changes,
d) updates safety and operational documentation,
e) ensure their testing before commissioning and
f) will ensure the possibility of returning to the original state.

(3) The obliged person based on the results of the risk assessment according to paragraph 2 letter b) decides on the implementation of penetration testing; if it decides to carry out penetration testing, it proceeds according to § 25 paragraph 6 of this decree.

§ 13

Acquisition, development and maintenance

Obliged person in connection with the planned acquisition, development and maintenance of assets

a) manages risks according to § 9,
b) governs significant changes according to § 12,
c) establishes security requirements in accordance with this decree and own security needs,
d) include the security requirements established under letter c) in the acquisition, development and maintenance project,
e) observes and enforces compliance with the requirements established under letter c),
f) ensure the separation of operational, backup, development, testing and other specific environments, and ensure the protection of information and data contained in them,
g) if the objective of the acquisition or development is a technical asset using an authentication mechanism , in particular for the purpose of verifying the identity of users or administrators, it meets the requirements according to § 20 paragraph 3 and
h) if the objective of the acquisition or development is a technical asset using cryptographic algorithms, it meets the requirements according to § 26 paragraph 1 letter a) and paragraph 3 letter and).

§ 14

Access control

(1) Based on security and operational needs, the obligated person manages access to assets and takes security measures that serve to ensure the protection of access and authentication data that are used for identity verification according to § 20 and § 21.

(2) Obliged person further within the framework of the management of access to assets

a) controls access based on groups and roles,
b) assign access rights and permissions and a unique identifier to each user and administrator accessing the assets,
c) manages the identifiers, access rights and authorizations of technical asset accounts,
d) implements security measures to control the access of technical assets to other assets,

e) implements the security measures required for the safe use of mobile devices and other similar technical assets, as well as security measures associated with the use of technical assets that the obligated person does not have under his control,
f) limit the allocation of administrative and privileged permissions to the level necessary to perform the job,
g) restrict and control the use of software resources and equipment that may be capable of bypassing system or application controls;
h) enforces that established rules and procedures are followed when using private authentication information and mechanisms,
i) assigns and removes access permissions in accordance with the access control policy,
j) performs a regular review of all access authorizations, including division into groups and roles,
k) ensure the immediate removal or change of access authorizations when changing position or classification based on groups and roles,
l) ensure the immediate removal or change of access authorizations upon termination or change of the contractual relationship,
m) documents the assignment and removal of access rights and
n) uses the tool for identity management and verification according to § 20 and the tool for managing access rights according to § 21.

§ 15

Management of cyber security events and incidents

(1) Mandatory person in the framework of the management of cyber security events and incidents
a) establish processes, rules and procedures for detecting, recording and evaluating cyber security events in accordance with § 22 to 24 and managing cyber security incidents,
b) will assign responsibilities for
1. detection, recording and evaluation of cyber security events and
2. coordination and management of cyber security incidents,
c) defines and adheres to rules and procedures for identifying, collecting, obtaining and preserving credible data needed for the analysis of a cyber security incident,
d) ensure the detection of cyber security events according to § 22,
e) ensure that users, administrators, persons holding security roles, other employees and suppliers report unusual behavior of technical assets and suspicions of any vulnerabilities,
f) provide for the assessment of cyber security events, during which a decision must be made as to whether they should be classified as cyber security incidents,
g) ensure the management of cyber security incidents according to established procedures,
h) takes security measures to prevent and mitigate the impact of a cyber security incident,
i) reports cyber security incidents according to § 16 of the Act,

j) keeps records of cyber security incidents and their management,
k) investigate and determine the causes of a cyber security incident and
l) evaluates the effectiveness of solving a cyber security incident and, based on the evaluation, determines the necessary security measures, or updates existing security measures to prevent the recurrence of the solved cyber security incident.

(2) The obliged person also uses the tools according to Sections 22 and 24 when detecting and evaluating cyber security events.

§ 16

Management of business continuity

(1) Mandatory person in the framework of business continuity management
a) establishes the methodology for carrying out the impact analysis,
b) evaluates and documents the possible impacts of cyber security incidents using an impact analysis and takes into account the risk assessment according to § 9, in which it assesses possible risks related to threats to the continuity of activities,
c) on the basis of the outputs of the impact analysis and risk assessment according to letter b) sets the objectives of managing the continuity of activities in the form of determination
1. the minimum level of services provided that is acceptable for the use, operation and management of the regulated service,
2. the recovery period during which the regulated service's minimum service level will be restored following a cyber security incident, and
3. data recovery point as the period of time during which data must be recovered after a cyber security incident or failure;
d) establishes a business continuity management policy, which includes the fulfillment of objectives according to letter c) and establishes the rights and obligations of administrators and persons holding security roles,
e) develop, update and regularly test business continuity plans and recovery plans related to the provision of the regulated service and
f) implements security measures to increase resistance according to § 27.

(2) Objectives of continuity management according to paragraph 1 letter c) of this provision are the specified time and quality of the regulated service according to § 34 of the Act. The specified time is the time to restore operation according to paragraph 1 letter c) point 2 of this provision and the established quality of the regulated service is the minimum level of services provided according to paragraph 1 letter c) point i) of this provision.

§ 17

Cyber security audit

(1) The obliged person establishes a plan for conducting a cyber security audit.

(2) Mandatory person in the framework of a cyber security audit
a) assesses whether the security measures required by the Cybersecurity Act and this decree have been implemented,
b) assesses the compliance of established security measures with legal regulations, internal regulations, other regulations, contractual obligations and best practice

related to the regulated service and

c) conducts and documents an audit of compliance with the rules and procedures set forth in the security policy, including a review of technical compliance and previously established corrective measures pursuant to paragraph 4.

(3) The obliged person shall take into account the results of the cyber security audit pursuant to paragraph 2 v

a) risk management plan,
b) statement of applicability a
c) security awareness development plan.

(4) The obliged person determines any corrective measures to meet the requirements according to paragraph 2.

(5) Cyber security audit according to paragraph 2 is carried out

a) in case of significant changes, within their scope,
b) at regular intervals at least after 2 years a
c) in accordance with the cyber security audit plan.

(6) If, in justified cases, it is not possible to conduct an audit in the interval according to paragraph 5 letter b) to the full extent according to paragraph 2, it is possible to conduct a cyber security audit continuously after systematic units. In such a case, the audit in its entirety according to paragraph 2 must be carried out within 5 years at the latest.

(7) The cyber security audit must be carried out by a person meeting the conditions set out in § 6 paragraph 4, who independently evaluates the correctness and effectiveness of the security measures in place.

TITLE II

TECHNICAL MEASURES

§ 18

Physical security

Mandatory person in the framework of physical security

a) prevents damage, theft, misuse of assets and interruption of regulated service,
b) establishes a physical security perimeter delimiting the area in which information and data are stored or processed, or in which the technical assets of the regulated service are located,
c) documents the individual physical security perimeters according to letter b) with regard to the evaluation of the located technical assets and divides them into individual levels of physical protection,
d) for each physical security perimeter established pursuant to letter c) shall adopt relevant security measures of physical protection with regard to its level of physical protection
    1. to prevent unauthorized access,
    2. to prevent damage and unauthorized interventions,
    3. to ensure physical protection at the level of objects and within objects,
    4. to ensure the detection of violations of the physical security perimeter and
    5. records entries and accesses to the physical security perimeter.

§ 19

Security of communication networks

Mandatory person for the protection of the security of the communication network, including its network perimeter

a) ensure the segmentation of the communication network, including the separation of operational, backup, development, testing and other specific environments,
b) will ensure communication management within the communication network,
c) will provide control of remote access to the communication network,
d) will ensure remote management of technical assets,
e) within the framework of communication control, remote access and remote administration, only such communication is permitted as is necessary for the proper provision of the regulated service,
f) using the cryptographic algorithms regulated in § 26 will ensure confidentiality and integrity in the transmission of information and data within the communication network and
g) uses a tool that ensures the protection of the integrity of the communication network.

§ 20

Management and verification of identities

(1) The obliged person uses a tool for managing and verifying the identity of administrators, users and technical assets of the regulated service.
(2) It provides a tool for managing and verifying the identity of administrators, users and technical assets
    a) identity verification before starting their activities,
    b) managing the number of possible failed login attempts,
    c) the resistance of stored and transmitted authentication data to threats and vulnerabilities that could compromise their confidentiality or integrity,
    d) re-verification of identity after a specified period of inactivity,
    e) maintaining confidentiality when creating default credentials and when restoring access a
    f) centralized management of identities with regard to links between assets.
(3) The obliged person to verify the identity of administrators, users and technical assets uses an authentication mechanism based on multi-factor authentication with at least two different types of factors.
(4) Until the requirements for verifying the identity of administrators, users or technical assets according to paragraph 3 are met, the obliged person keeps records of technical assets, accounts and authentication mechanisms that do not meet these requirements, including justification.
(5) Until the requirement to verify the identity of administrators, users or technical assets using an authentication mechanism based on multi-factor authentication with at least two different types of factors according to paragraph 3 is met, the obliged person uses authentication using

cryptographic keys or certificates.

(6) Until the requirement to verify the identity of administrators, users and technical assets using an authentication mechanism based on authentication using cryptographic keys or certificates according to paragraph 5 is met, the obligated person uses a tool based on authentication using an account identifier and password, and this tool must enforce the following rules
    a) password length at least
        1. 12 characters for user accounts,
        2. 17 characters for administrator accounts,
        3. 22 characters for technical asset accounts,
    b) allowing you to enter a password of at least 64 characters,
    c) unrestricted use of lower and upper case letters, numbers and special characters,
    d) allowing users and administrators to change their password, while the period between two password changes must not be shorter than 30 minutes,
    e) mandatory password changes at intervals of no more than 18 months,
    f) disallowing users and administrators
        1. choose simple and frequently used passwords,
        2. create passwords based on multiple characters, login name, email, system name or similar and
        3. reuse of previously used passwords with a memory of at least 12 previous passwords.

(7) Obliged person in accordance with paragraph 6
    a) generates a random default password or identifier used to create or restore access and
    b) ensure the immediate change of the default password of the technical asset,
    c) ensure that users and administrators promptly change their default passwords after first login,
    d) ensure that as part of the verification of the identity of the technical asset, its new password is generated by a random string consisting of upper and lower case letters, numbers and special characters, and
    e) shall immediately force the change of the access password in case of reasonable suspicion of its compromise.

(8) The obliged person shall immediately invalidate the password or identifier used to create or restore access after its first use or after a maximum of 24 hours have passed since its creation.

(9) The obliged person for the administrator account intended especially for the case of recovery after a cyber security incident must enforce the following rules
    a) immediately force a default password change,
    b) the password must be made up of a random string consisting of uppercase and lowercase letters, numbers and special characters,
    c) password length must be at least 22 characters,
    d) the password must be stored securely,
    e) persons can manipulate the account and its password in absolutely necessary cases,
    f) a password change must be enforced after its use, upon any change of responsible persons or at an interval of no more than 18 months, and
    g) records manipulation and manipulation attempts with this account and its

password.

§ 21

Management of access rights

Mandatory person for managing access rights

a) uses a centralized tool with regard to the links between assets,
b) controls the authorization to access individual assets and
c) controls permissions to read data, write data, and change permissions.

§ 22

Detection of cyber security events

(1) The obliged person uses a tool for the detection of cyber security events, which he provides within the communication network
   a) verification and control of transmitted data within the communication network and between communication networks,
   b) verification and control of transmitted data on the network perimeter of the communication network and
   c) blocking unwanted communication.
(2) The obliged entity uses a centrally managed tool with regard to the links between assets for the detection of cyber security events, which ensures for individual relevant technical assets
   a) continuous and automatic protection against malicious code,
   b) management and monitoring of the use of removable devices and data carriers,
   c) control of the automatic launch of content, especially for removable devices and data carriers,
   d) controlling permissions to execute code,
   e) managing and monitoring the communication of applications, their services and processes,
   f) detection of cyber security events over technical assets and
   g) detection based on the behavior of the technical asset, administrators and users.
(3) The obliged person shall regularly and promptly update the tool used in accordance with paragraphs 1 and 2, including its settings and detection rules.

§ 23

Recording of events

(1) Based on the assessment of assets and security needs, the obliged person shall determine the technical assets for which the recording of security and relevant operational events is carried out.
(2) In accordance with paragraph 1, the obliged person records safety and relevant operational events
   a) detected according to § 22,
   b) within the communication network,

c) on the network perimeter and
d) technical assets.

(3) The obliged person shall update the range of technical assets determined pursuant to paragraph 1 at regular intervals and upon significant changes.

(4) The obliged person ensures continuous synchronization of the uniform time of technical assets.

(5) As part of recording events according to paragraph 2, the obliged person records in particular the following information about the event
a) date and time including time zone specification,
b) type of activity,
c) unambiguous identification of the technical asset that recorded the activity,
d) unambiguous identification of the account under which the activity was carried out,
e) unambiguous identification of the device of the originator and
f) success or failure of the activity.

(6) The obliged person shall ensure a unique network identification according to paragraph 5 letter c) to e) in the event that this network identification changes in the communication network.

(7) As part of ensuring the confidentiality and integrity of the information obtained pursuant to paragraph 2, the obliged person shall ensure its protection against unauthorized reading and any change.

(8) As part of the recording of events according to paragraph 2, the obliged person, in particular, records
a) logging in and out of all accounts, including failed attempts,
b) performing and unsuccessfully attempting to perform a privileged activity,
c) manipulation and unsuccessful attempt to manipulate accounts, authorizations and rights,
d) failure to perform activities due to lack of access rights or authorization,
e) initiation and termination of technical asset activities,
f) critical and error reports of technical assets,
g) access and unsuccessful attempt to access event logs,
h) manipulation and unsuccessful attempt to manipulate event records,
i) change and failed attempt to change event logging tools settings and
j) other user activities that may affect the security of the regulated service.

(9) The obliged person shall use a central tool with regard to the links between the assets for the collection and storage of records of the events recorded in accordance with paragraph 2.

(10) The obliged person shall keep records of events recorded pursuant to paragraph 2 for at least 18 months.

§ 24

Evaluation of cyber security events

(1) The obligated person uses a tool for the continuous evaluation of cyber security events detected pursuant to § 22 for
a) collecting, searching and grouping related records for the purpose of detecting

cyber security events,

b) continuous provision of information about detected cyber security events, early warning of designated security roles and

c) evaluating cyber security events with the aim of identifying cyber security incidents.

(2) As part of the use of the instrument, the obliged person shall ensure in accordance with paragraph 1

a) limiting cases of incorrect or unwanted evaluation of cyber security events,

b) regularly updating the tool's settings, including its rules for detecting and evaluating cyber security events and

c) regular updating of rules for continuous provision of information about detected cyber security events, including early warning of designated security roles.

(3) The obliged person uses the information obtained by the tool for evaluating cyber security events for the optimal setting of the information security management system of the regulated service and the implementation of security measures.

§ 25

Application security

(1) The person obliged to ensure the security of the regulated service uses technical assets that are supported by the manufacturer, supplier or other person and ensures the immediate application of security updates issued for these assets.

(2) By the time paragraph 1 is fulfilled, the obliged person shall register technical assets that are no longer supported by the manufacturer, supplier or other person and implement security measures that guarantee a similar or higher level of security of these technical assets.

(3) Furthermore, as part of application security, the obligated person shall ensure permanent protection of applications, information, transactions and transmitted session identifiers from

a) unauthorized activity and

b) by denying the actions taken.

(4) The obliged person performs regular vulnerability scanning of the technical assets of the regulated service

a) from the internal and external communication network and

b) at least once a year.

(5) The obliged person takes into account the results of vulnerability scans as part of risk management according to § 9 and implements security measures based on the results found.

(6) The obliged person performs penetration testing of technical assets with regard to the assessment of these assets and risk assessment

a) from the internal and external communication network,

b) before their commissioning and

c) in connection with a significant change according to § 12 paragraph 3.

(7) The obliged person takes into account the results of penetration testing as part of risk management according to § 9 and implements security measures based on the results found.

(8) The obliged person will perform a retest (retest) of the finding established on the basis of the performed vulnerability scan or penetration testing in order to verify the functionality of the established security measures.

(9) Obliged person in accordance with paragraph 6 letter a) performs regular penetration testing at least once every two years.

(10) In justified cases, if he cannot perform penetration testing in the scope or interval specified in paragraph 9, he may divide this penetration testing into systematic units. In such a case, it is necessary to carry out penetration testing to the extent specified in paragraph 6 within 5 years at the latest.

§ 26

Cryptographic algorithms

(1) Mandatory person for ensuring the protection of technical assets and their communication
   a) uses currently robust cryptographic algorithms,
   b) promotes safe handling of cryptographic algorithms and
   c) takes into account recommendations and methodologies in the field of cryptographic algorithms issued by the Office, published on its website.

(2) In accordance with paragraph 1, the obliged person ensures safe
   a) voice, audiovisual and text communication, including e-mail communication and
   b) emergency communication within the organization.

(3) In the case of the use of cryptographic keys and certificates for the protection of technical assets and communication networks, the obliged person uses
   a) only currently resistant cryptographic keys and certificates and
   b) a key and certificate management system that
      1. ensure the generation, distribution, storage, changes, limitation of validity, invalidation of certificates and proper disposal of cryptographic keys,
      2. enable control and audit and
      3. ensure the confidentiality and integrity of cryptographic keys.

§ 27

Ensuring the availability of a regulated service

(1) The obliged person shall implement security measures to ensure the availability of the regulated service, which they shall ensure
   a) the availability of the regulated service according to the objectives set in accordance with § 16,
   b) the resilience of the regulated service to threats and vulnerabilities that could reduce its availability and
   c) redundancy of assets necessary to ensure the availability of the regulated service.

(2) The person obliged to ensure the availability of the regulated service in accordance with paragraph 1 creates regular backups of technical asset settings, information and data necessary in particular for the purpose of restoring the regulated service in the event of a cyber security incident.

(3) In the case of advances made pursuant to paragraph 2, the obligated person shall ensure
   a) regular testing of their integrity, availability and recoverability,
   b) documenting the results of the tests carried out in accordance with paragraph 3

letter and),

c) protection of stored backups and the data contained in them against violations of their integrity and confidentiality, in particular by encrypting these backups in accordance with § 26 and

d) protection of stored backups and the data contained in them against disruption of their availability.

(4) In order to limit the spread of a cyber security incident and reduce its impact, the obliged person separates the backup environment from other environments in accordance with § 19 letter and).

§ 28

Security of industrial, management and similar specific technical assets

The obliged person to ensure the cyber security of industrial, management and similar specific technical assets further uses tools and implements security measures that ensure

a) limitation of physical access to industrial, management and similar specific technical assets,

b) restriction of authorization to access industrial, management and similar specific technical assets,

c) segmentation of communication networks of industrial, control and similar specific technical assets from other environments and segmentation of these communication networks according to § 19,

d) limitation of remote accesses and remote management of industrial, control and similar specific technical assets,

e) protection of individual industrial, management and similar specific technical assets against the use of threats and known vulnerabilities and

f) restoring the availability of industrial, management and similar specific technical assets.

PART THREE

FINAL PROVISIONS

§ 29

Transitional provisions

Providers of a regulated service who, on the day preceding the entry into force of this decree, were an authority or a person pursuant to § 3 of Act No. 181/2014 Coll., on cyber security, which imposes obligations in the area of introduction and implementation of security measures pursuant to Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, submission requirements in the field of cyber security and data disposal (decree on cyber security), as amended before the date of entry into force of this decree, and who fulfill the criteria on the date of entry into force of this decree for the identification of at least one regulated service, implements and implements security measures in accordance with Decree No. 82/2018 Coll., on security measures, cyber security incidents , reactive measures, submission requirements in the field of cyber security and data disposal (decree on cyber security), in the version effective before the date of entry into force of this decree.

PART FOUR

EFFECTIVENESS

§ 30

Effectiveness

This decree becomes effective on dd.mm.yyyy .

Director:
Ing. Lukáš Kintr incl

Annex No. 1 to Decree No. XX/XXXX Coll.

Asset identification and valuation

1) When identifying the primary assets of a regulated service, it is appropriate to first identify its purpose. It is possible to derive a service type asset from the purpose. Subsequently, it is appropriate to identify what information the given service works with and derive the primary assets of the information type.
2) When identifying supporting assets, it is necessary to start from the architecture of the system of the regulated service and, in particular, take into account the links to primary assets. The obliged entity should choose such a detail of the supporting assets that it is able to adequately identify and manage the risks associated with the assets.
3) Asset guarantors are determined based on their job title and process and asset expertise. For asset management purposes, the guarantor of the asset must be able to value the asset based on possible impacts.
4) In this case, the four-level scales shown in tables No. 1, 2 and 3 are used to evaluate the assets, and the impact of a breach of information security for individual assets is assessed. It is recommended that the liable person adapts these asset rating levels in the scale to his needs. The obliged entity may use a different number of asset rating levels than that specified in this Annex, provided it maintains clear links between the asset rating method used and the asset rating scales and levels specified in this Annex.
5) In the case of primary assets, it is also necessary to take into account at least the areas listed in Table No. 4 - Areas of evaluation of primary assets.
6) When evaluating supporting assets, it is necessary to take into account the links between supporting and primary assets. One of the following variants can be used, for example
   a) supporting assets take over the values of primary assets,
   b) supporting assets are assessed individually with regard to the value of primary assets,
   c) the supporting assets take on the values of the primary assets through an appropriately chosen formula.
7) Asset protection rules also apply to paper documents, removable devices and data carriers that are electronic copies of the originals.

Tab. No. 1: Confidentiality Rating Scale

Level	Description	Examples of asset protection requirements
Low	The assets are publicly available or have been intended to be publicly available. Violation of the confidentiality of assets does not threaten the legitimate interests of the obligated person.	No protection required. In the case of sharing such an asset with third parties and using the so-called traffic classification light protocol (hereinafter referred to as "TLP"), the designation TLP:CLEAR is used . Liquidation/deletion of an asset at the Low level - see Appendix No. 4.
Medium	The assets are not publicly accessible and constitute the know-how of the liable party, asset protection is not required by any legal regulation or contractual agreement.	Access control tools are used to protect confidentiality. In the case of sharing such an asset with third parties and using the TLP classification, the designation TLP:GREEN or TLP:AMBER is used in particular. Liquidation/deletion of an asset at the Medium level - see Appendix No. 4.
High	Assets are not publicly accessible and their protection is required by law, other regulations or contractual agreements (for example, trade secrets, personal data).	To protect confidentiality, means are used to ensure control and logging of access. Information transmissions through communication networks are protected using cryptographic means. In the case of sharing such an asset with third parties and using the TLP classification, the designation TLP:AMBER or TLP:AMBER+STRICT is used in particular. Liquidation/deletion of an asset at the High level - see Appendix No. 4.
Critical	The assets are not publicly accessible and require a higher level of protection than the previous category (for example, strategic trade secrets, special categories of personal data).	To protect confidentiality, means are used to ensure control and logging of access. Furthermore, protection methods preventing abuse of assets by administrators. Information transmissions are protected using cryptographic means. In the case of sharing such an asset with third parties and using the TLP classification, the designation TLP:RED is used in particular . Liquidation/deletion of an asset at the Critical level - see Appendix No. 4.

Tab. No. 2: Integrity Rating Scale

Level	Description	Examples of asset protection requirements
Low	The asset does not require integrity protection. Violation of the integrity of the asset does not threaten the legitimate interests	No protection required.

	of the obligee.	
Medium	An asset may require integrity protection. Violation of the integrity of the asset may lead to damage to the legitimate interests of the obligee and may manifest itself in less serious impacts on the primary assets.	Standard tools are used to protect integrity.
High	The asset requires integrity protection. Violation of the integrity of the asset leads to damage to the legitimate interests of the obligee with substantial impacts on the primary assets.	To protect integrity, special tools are used that allow you to track the history of changes made and record the identity of the person making the change. Protection of the integrity of information transmitted by communication networks is ensured by means of cryptographic means.
Critical	The asset requires integrity protection. Violation of integrity leads to very serious damage to the legitimate interests of the obligated person with direct and very serious impacts on primary assets.	To protect integrity, special means of unambiguous identification of the person making the change are used.

Tab. No. 3: Accessibility Rating Scale

Level	Description	Examples of asset protection requirements
Low	Disruption of the availability of the asset is not important and in the event of an outage a longer period of time for rectification (approx. up to 1 week) is normally tolerated.	Regular backups are sufficient to protect availability.
Medium	Disruption of the asset's availability should not exceed the duration of a working day, a longer-term outage leads to a possible threat to the legitimate interests of the obligee.	Common backup and recovery methods are used to protect availability.
High	Disruption of asset availability should not exceed a few hours. Any shortfall must be dealt with immediately, as it leads to a direct threat to the legitimate interests of the obligee. Assets are considered very important.	Back-up systems are used to protect availability, and the restoration of service provision may be conditioned by operator intervention or replacement of technical assets.
Critical	Violation of the availability of the asset is not permissible , even short-term unavailability (in the order of a few minutes) leads to a serious threat to the legitimate	Backup systems are used to protect availability, and the restoration of service provision is short-term and automated.

	interests of the liable person. Assets are considered critical.	

Tab. 4 Areas of assessment of primary assets

When evaluating primary assets, it is necessary to assess at least the relevant of the following areas

Region	Example
a) scope and importance of personal data, special categories of personal data	Leakage of personal data of a natural person.
b) the extent of the legal obligations or other obligations or trade secrets concerned	Violation of the obligation to publish documents on the electronic official board, which must be continuously accessible by remote access. Breach of contract and the resulting sanctions. Leakage of trade secrets. Violation of legislation and resulting fines.
c) extent of disruption of internal management and control activities	Incompleteness or modification of information needed for management decision-making and control activities.
d) damage to public, commercial or economic interests and possible financial losses	Unavailability of information about invoices based on the unavailability of the economic system. Unavailability of information about possible business opportunities and resulting lost profit. The unavailability of e.g. websites can lead to not informing the public about important facts (floods, ecological disasters, etc.).
e) impacts on the provision of important services	Disruption of all information and services related to the regulated service and the main business goal (purpose of existence) of the organization.
f) extent of disruption of normal activities	Disruption of personnel, economic, building and fleet management activities, inability to receive data messages, etc.
g) effects on the preservation of good name or the protection of good reputation	Default. Leakage of internal information.
h) impacts on the safety and health of persons	Inability to provide basic income, food, access to health care, freedom, etc. Possibility of injury and loss of life.
i) impacts on international relations	Leakage of information from foreign partners. Leakage of information from a partner who is part of an international concern.
j) impacts on users of the information and communication system	Loss of the user's ability to access the service due to its unavailability.

Annex No. 2 to Decree No. XX/XXXX Coll.

Risk assessment

1) Unambiguous determination of the function for risk determination is a necessary part of the risk assessment methodology according to § 9 of this decree.
2) Value at risk is most commonly expressed as a function of asset value, threat, and vulnerability.
3) For example, the following function can be used for risk assessment: Risk = Asset Value × Threat × Vulnerability.
4) In this case, the value of the asset is derived from the assessment of assets according to Annex No. 1 of this decree.
5) to merge the threat and vulnerability assessment scales , i.e. create scenarios combining threat and vulnerability. Merging the scales should not result in a loss of ability to differentiate threat and vulnerability levels. For this purpose, for example, a comment can be used that clearly expresses both the threat level and the vulnerability level. The procedure is similar in cases where the obliged entity uses a different number of levels for the values of assets, threats, vulnerabilities and risks.

Tab. #1: Threat Rating Scale

Level	Description
Low	The threat does not exist or is unlikely. The predicted realization of the threat is no more frequent than once every 5 years.
Medium	The threat is unlikely to likely. The expected realization of the threat is in the range from 1 year to 5 years.
High	The threat is likely to very likely. The expected realization of the threat is in the range from 1 month to 1 year.
Critical	The threat is very likely to more or less certain. The expected realization of the threat is more frequent than once a month.

Tab. No. 2: Vulnerability Rating Scale

Level	Description
Low	The vulnerability does not exist or the vulnerability is unlikely to be exploited. Security measures are in place that are able to detect potential vulnerabilities or possible attempts to exploit them in time.
Medium	Exploitation of the vulnerability is unlikely to likely. Security measures are in place, the effectiveness of which is regularly checked. The ability of security measures to detect possible vulnerabilities or possible attempts to overcome security measures in time is limited. There are no known successful attempts to bypass the security measures.
High	Exploitation of the vulnerability is likely to very likely. Safety measures are in place, but their effectiveness does not cover all the necessary aspects and is not regularly checked. Partially successful attempts to overcome security measures are known.

Critical	Exploitation of the vulnerability is very likely to more or less certain. Safety measures are not implemented or their effectiveness is greatly limited. The effectiveness of security measures is not being checked. Successful attempts to overcome security measures are known.

Tab. No. 3: Scale for risk assessment

Level	Description
Low	The risk is considered acceptable.
Medium	The risk can be reduced by less demanding security measures or, in the case of more demanding security measures, the risk is acceptable.
High	The risk is unacceptable in the long term and systematic steps must be taken to eliminate it.
Critical	The risk is unacceptable and steps must be taken to eliminate it immediately.

6) If the risk value is higher than the acceptability limit, appropriate security measures should be implemented to reduce the risk value or eliminate the risk and ensure the required level of information security. The methods for risk management are as follows
   a) risk acceptance,
   b) risk reduction and elimination,
   c) risk avoidance, or
   d) transfer or sharing of risk.

Annex No. 3 to Decree No. XXXX Coll.

Vulnerabilities and threats

Warning: This appendix contains only selected categories of vulnerabilities and threats. The obliged person identifies specific threats and vulnerabilities according to his needs and specifics. Identification of specific vulnerabilities and threats is the responsibility of the obligated person.

Vulnerabilities

1. insufficient maintenance of assets,
2. obsolescence of assets,
3. insufficient perimeter protection,
4. insufficient security awareness of users, administrators, persons holding security roles, suppliers and senior management,
5. insufficient backup,
6. inappropriate setting of access permissions,
7. insufficient procedures and processes for detecting cyber security events and identifying cyber security incidents,
8. insufficient monitoring of user and administrator activity and failure to detect activity that may affect the security of the regulated service
9. insufficient determination of security rules and procedures, imprecise or ambiguous

definition of the rights and obligations of users, administrators, persons holding security roles, suppliers and senior management,
10. insufficient asset protection,
11. inappropriate security architecture
12. insufficient degree of independent control,
13. the inability of users, administrators, security role holders, suppliers and senior management to detect misconduct in a timely manner;
14. lack of employees with the necessary professional level of knowledge,
15. placing the asset outside of physical control (e.g. on the territory of a foreign state),
16. location of the asset on the territory of a state whose legal environment the liable person is not sufficiently aware of,
17. vulnerabilities discovered during vulnerability scanning and penetration testing.

Threats

1. violation of security policy, execution of unauthorized activities, abuse of authorization by users, administrators, persons holding security roles, suppliers and senior management,
2. damage or failure of technical or software equipment,
3. identity theft,
4. use of the software in violation of the license terms,
5. malicious code
6. breach of physical security,
7. interruption of the provision of electronic communications services or electricity supplies,
8. misuse or unauthorized modification of information,
9. loss, theft or damage to an asset,
10. non-compliance with the contractual obligation on the part of the supplier,
11. misconduct by users, administrators, security role holders, suppliers and senior management;
12. misuse of internal resources, sabotage,
13. long-term interruption of the provision of electronic communications services, the supply of electricity or other important services,
14. employees with an insufficient professional level of knowledge,
15. targeted cyber attack using social engineering, use of espionage techniques,
16. misuse of replaceable technical data carriers,
17. attack on electronic communication (eavesdropping, modification),
18. dependence on suppliers,
19. abuse of state power to access assets,
20. making available or handing over assets at the request of the state.

Annex No. 4 to Decree No. XXXX Coll.

Disposal of data

1) This annex specifies the obligee's obligations to define the methods of disposal of

information and data and their copies and the disposal of technical assets that are carriers of information and data with regard to the level of assets.

2) The obligated person shall establish rules for the method of disposal of information and data and their copies and disposal of technical assets that are carriers of information and data in accordance with this annex. This does not affect obligations under other legal regulations. It is necessary to choose an adequate level of service offering adequate security measures, including adequate rules for the disposal of information, data and technical assets that are carriers of information and data with respect to the level of assets.
3) Rules for the disposal of information and data should be set in proportion to the level of assets and should in particular take into account
   a) the value of the asset (especially from a confidentiality perspective),
   b) technology (types and sizes of information and data carriers),
   c) whether the carrier of information and data is under the control of the organization or not,
   d) whether the information and data are part of a dedicated or shared environment,
   e) who will dispose of the information and data (e.g. an internal employee or supplier),
   f) availability of disposal equipment and tools,
   g) the capacity of liquidated information and data carriers,
   h) whether trained personnel are available,
   i) the time required for liquidation,
   j) the cost of disposal with regard to tools, training, validation and reuse of the information and data carrier
   k) possible ways of disposing of information and data (for example, by destroying the carrier, overwriting the carrier of information and data several times, erasing, encryption, etc.),
   l) applicable methods of disposal of information and data due to the state of the information carrier (for example, if the device is damaged, it will not be possible to use the option of overwriting the data, but one of the methods of physical disposal).
4) Methods of disposal of information and data and technical assets that are carriers of information and data and their copies
   i) Removal
      1) The method of disposing of information and data carriers so that they are unavailable (for example, deleting a data file, throwing a printed document into the trash).
      2) This is the least secure way of disposing of information and data. In the event that the information and data carrier is obtained, it is possible to restore the information and data with some effort.
      3) This method is not applicable to non-rewritable digital information and data carriers.
      4) Applicable method for asset confidentiality level (based on Annex No. 1): low.
   j) Overwriting
      1) The disposal method consists in repeatedly overwriting information and data with random values.

2) It is a moderately secure way of disposing of information and data. Freely available tools do not allow recovery of overwritten information and data.

3) Overwriting can be replaced or combined with secure disposal of cryptographic keys to encrypted information.

4) This method is not suitable for damaged media, non-rewritable media, or media with a large capacity.

5) Applicable method for asset confidentiality level (based on Annex No. 1): low to critical.

k) Physical disposal of information and data carriers

1) The method of disposal consists in the destruction of the information and data carrier, or in the disassembly of the device and the subsequent destruction of the information and data carrier (by mechanical, chemical or thermal action).

2) It is the most secure method of disposing of information and data. The carrier of information and data after physical disposal cannot be reused for its original purpose. The original information and data cannot be restored even with a great deal of resources and effort.

3) Applicable disposal method for asset confidentiality level (based on Annex No. 1): medium to critical.

Example of possible methods of liquidation according to the level of confidentiality of the asset (based on Appendix No. 1)

<table>
<tr><td></td><td colspan="4">Permissible method of liquidation by asset level</td></tr>
<tr><td>Carrier of information</td><td>1. Low</td><td>2. Medium</td><td>3. High</td><td>4. Critical</td></tr>
<tr><td rowspan="2">Information and data on a human-readable medium (printed documents, notes and others).</td><td rowspan="2">Disposal: Dispose of in the waste.</td><td>Rewrite: Blackening.</td><td colspan="2" rowspan="2">Physical disposal: Degradation of the information and data carrier by using a shredding machine with longitudinal and transverse cutting, burning or disassembly.</td></tr>
<tr><td>Physical disposal: Destruction of information and data carriers using a shredding machine.</td></tr>
<tr><td>Mobile devices (mobile phones, tablets, laptops and others).</td><td>Removal: Erasing information and data, resetting the device to factory settings.</td><td>Rewrite: For devices with encrypted storage - delete information and data and reset to factory settings.</td><td colspan="2" rowspan="3">Physical disposal: Disassembly of the device and destruction of the information and data carrier.</td></tr>
<tr><td>Network devices (router, switch, modem and others).</td><td rowspan="2">Removal: Erasing information and data, resetting to factory settings.</td><td rowspan="2">Rewrite: Removal and flooding of artificial events (artificial network traffic, test print jobs, etc.).</td></tr>
<tr><td>Office equipment (scanners ,</td></tr>
</table>

<table>
<tr><td>printers, fax)</td><td></td><td></td><td colspan="2"></td></tr>
<tr><td rowspan="2">Internal and external memories (magnetic tapes, HDD, SSD, CD, DVD, removable media and others).</td><td rowspan="2">Deletion: Deleting information and data at the file system level.</td><td>Rewrite: Overwriting information and data. In the case of encrypted media, an alternative is the safe disposal of cryptographic keys</td><td colspan="2" rowspan="2">Physical disposal: Destruction of the carrier of information and data.</td></tr>
<tr><td>Physical disposal.</td></tr>
<tr><td rowspan="3">Outsourcing and the cloud</td><td colspan="4">The permissible method of disposal of information and data should be determined by contractual agreement.</td></tr>
<tr><td>Removal: Deleting all files including previous versions.</td><td>Rewrite: Use of storage media level encryption and secure disposal of cryptographic keys.</td><td rowspan="2">Rewrite: Use of storage media level encryption and secure disposal cryptographic keys stored in a certified hardware security module (HSM) controlled by the customer (for example, according to the FIPS 140-2 Level 2 standard). Upon termination of service, the master access key will be disposed of and information and data overwritten.</td><td rowspan="2">Overwriting/ Physical Disposal: Use method see level “3. High” or dedicated storage memory capacity used. At the end of the service, a total sanitization of all used storage media was carried out according to the above lines for the critical level.</td></tr>
<tr><td></td><td>Alternatively, in the case of a dedicated storage medium, information and data can be overwritten after the service is terminated.</td></tr>
</table>

Annex No. 5 to Decree No. XXXX Coll.

Content of security policy and security documentation

1. Security policy
   1.1. Information Security Management System Policy
   a) Objectives, principles and needs of the information security management system.
   b) The scope and boundaries of the information security management system.
   c) Rules and procedures for planning, managing and recording the activity of human and technical resources of the information security management system.
   d) Rules and procedures for evaluating the effectiveness and reviewing the information security management system.

e) Rules and procedures for corrective actions and improvement of the information security management system.

1.2. Organizational security policy

a) Determining the composition of the Cyber Security Management Committee and its rights and obligations.

b) Determination of security roles and their rights and obligations.

c) Determining the rights and obligations of users and administrators.

d) Requirements for separation of performance of activities of individual security roles.

e) Requirements to separate performance of security and operational roles.

1.3. Security policy management policy and documentation

a) Designation of a person responsible for regular review and updating of security policies and security documentation.

b) Rules and procedures for reviewing and updating security policies and security documentation.

1.4. Asset Management Policy

a) Asset management process.

b) Responsibilities for the asset management process.

c) Protection rules for individual asset levels

1) permissible ways of using assets,

2) asset handling rules,

3) rules for classification of information,

4) asset tagging rules,

5) exchangeable media management rules,

6) rules for secure electronic sharing and physical transfer of assets, and

7) rules for determining the method of disposal of data, operational data, information and their copies or disposal of technical data carriers with regard to the level of assets.

d) Personal data protection rules and procedures.

1.5. Risk management policy

a) Risk management process.

b) Responsibilities for the risk management process.

1.6. Supplier Management Policy

a) Rules and principles for the selection of suppliers.

b) Rules for evaluating risks related to suppliers.

c) Rules and principles for determining significant suppliers.

d) The requirements of the contract taking into account the relevant requirements for suppliers resulting from security policies and security documentation.

e) Necessities of the contract on the level of services and the method and level of implementation of security measures and the determination of mutual contractual responsibility.

f) Rules for conducting control of the implementation of security measures.

g) Rules for evaluation of suppliers.

h) Rules for keeping records of contact data of suppliers entrusted with the performance of system and technical support.

i) Rules for eliminating dependence on one supplier (especially the issue of vendor lock -in and exit strategy).

1.7. Human resource security policy

a) Rules and procedures for the development of security awareness and methods of its evaluation
   1) ways and forms of teaching and training users,
   2) methods and forms of instruction and training of administrators,
   3) methods and forms of instruction and training of persons holding security roles,
   4) methods and forms of instruction and training of top management
   5) ways and forms of instructing suppliers

b) Safety training for new employees.

c) Setting deadlines for regular refresher training for users, administrators, people in security roles and senior management.

d) Rules and procedures for handling cases of violations of the security policy of the information security management system.

e) Rules and procedures for termination of employment or change of job position
   1) return of entrusted assets and withdrawal of rights upon termination of the employment relationship,
   2) change of access rights when changing job position.
   3) handing over responsibilities when changing job positions or terminating employment with administrators or persons holding security roles

f) Rules of basic cyber hygiene.

g) Rules for creating and using passwords.

h) Rules and procedures for checking compliance with security policies.

i) How to keep track of trainings.

1.8. Policy for safe behavior of users, administrators and persons holding security roles

a) Rules and procedures for safe handling of technical assets.

b) Rules and procedures for safe handling of access passwords and other authentication mechanisms.

c) Rules and procedures for secure use of e-mail and Internet access.

d) Rules and procedures for secure remote access.

e) Rules and procedures for safe behavior on the Internet and social networks.

f) Rules and procedures for reporting unusual behavior of technical assets and suspicions of any vulnerabilities.

1.9. Mobile Safe Use Policy

a) Rules and procedures for the safe handling and use of mobile devices in the internal communication network and beyond.

b) Rules and procedures for ensuring the security of devices that the obligated person does not have under their control (BYOD security).

1.10. Change management policy

a) Change management rules and procedures.

b) Rules and procedures for determining and approving changes that have or may affect cybersecurity.

c) Rules, procedures and criteria for reviewing the impact of changes to determine

significant changes.

d) Rules and procedures for assessing risks associated with significant change and selecting security measures.

e) Rules and procedures for managing significant changes.

f) Method of keeping records of significant changes.

g) Rules and procedures for testing significant changes before they are put into operation, including the possibility of returning to the original state (so-called rollback).

h) Rules and procedures for deciding to perform penetration testing.

1.11. Acquisition, Development and Maintenance Policy

a) Security requirements for acquisition, development and maintenance.

b) Security requirements for the separation of operational, backup, development, test and other specific environments within acquisition, development and maintenance.

c) Security requirements for multi-factor authentication.

d) Security requirements for cryptographic algorithms.

e) Security requirements with regard to the use of the zero trust principle .

f) Security requirements for vulnerability management in acquisition, development and maintenance.

g) Rules and procedures for deployment and installation of technical assets.

h) Software and information licensing and acquisition policy

1) rules and procedures for deploying software and its records,

2) rules and procedures for checking compliance with license conditions.

1.12. Access control policy

a) Rules and procedures for working with the tool used for managing and verifying identities and tools governing access rights and defining the responsibilities of responsible persons.

b) Rules and procedures for access control and authorization control, including the use of least privilege and need to know principles .

c) Life cycle of access control and determination of persons responsible for individual phases.

d) Life cycle of authorization management and determination of persons responsible for individual phases.

e) Rules and procedures for managing privileged and administrative privileges.

f) Emergency Access Control Rules and Procedures

g) Rules, procedures and records for accounts used especially for recovery after a cyber security incident.

h) Regular review of access rights, including the division of individual users into access groups.

i) Rules, procedures and requirements for managing access to technical assets under management and technical assets outside the management of the liable person.

j) Rules for authentication mechanisms and password policies.

1.13. Policy for handling cyber security events and incidents

a) Defining a cyber security event and a cyber security incident.

b) Rules and procedures for continuous detection, recording and evaluation of cyber security events.

c) Rules and procedures for identifying and managing cyber security incidents

d) Rules and procedures for the identification, collection, acquisition and preservation of credible evidence needed for the analysis of a cyber security incident.

e) Rules and procedures for testing set policies and procedures for handling cyber security incidents.

f) Rules and procedures for reporting unusual behavior of technical assets and suspicions of any vulnerabilities.

g) Rules and procedures for evaluating, solving and determining the cause of solving cyber security incidents and for regularly updating the rules for evaluating cyber security incidents.

h) Cyber Security Incident Reporting.

i) Logging of cyber security incidents .

1.14. Business Continuity Management Policy

a) Rights and obligations of responsible persons.

b) Business continuity management objectives for individual services

   1) the minimum level of services provided,

   2) recovery time,

   3) data recovery point.

c) Prioritization of individual services.

d) Methods of crisis communication and reporting.

e) Communication matrix with key persons for individual services.

f) Escalation procedures for crisis situations.

g) Catalog of scenarios of crisis situations.

h) Procedures for starting and stopping the system, for restarting or resuming the system after a failure, and for handling error conditions or extraordinary phenomena.

i) Method and period of testing individual business continuity plans and recovery plans.

j) Procedures for the implementation of measures issued by the Office.

1.15. Physical Security Policy

a) Determination of physical security perimeters and their level.

b) Rules and procedures for the protection of individual levels of physical security perimeters.

   1) Rules and procedures for checking and recording the entry of persons.

   2) Rules and procedures for the protection of facilities and located assets.

   3) Rules and procedures for detecting breaches of physical security.

1.16. Communication network security policy

a) Rules and procedures for ensuring network segmentation and separation of individual environments.

b) Rules, rights and permissions for individual segments and environments with respect to allowing only necessary communication.

c) Determining the rights and obligations for managing the secure operation of the communication network.

d) Rules and procedures for managing communication in a communication network.

e) Rules and procedures for controlling remote access to the communications network, including remote access by suppliers or others.

f) Rules and procedures for remote management of technical assets, including remote management of technical assets by a supplier or other persons.

1.17. Event Logging Policy

a) Defining the scope, the periodicity of updating the scope of technical assets and determining the person responsible for the up-to-dateness of this scope.

b) Rules and procedures for connecting technical assets to a tool used to collect event records.

c) Rules and procedures for the unambiguous identification of technical assets for the unambiguous determination of the originator of the recorded event.

d) Rules and procedures for the collection, recording and storage of safety and relevant operational events.

e) Rules and procedures for recording the activity of administrators, suppliers and other privileged accounts.

f) Rules and procedures for uniform time synchronization of technical assets.

g) Rules for the retention of recorded events.

1.18. Policy on the deployment, use and maintenance of tools for the detection of cyber security events and tools for the collection and evaluation of cyber security events

a) Rules and procedures for deploying tools for the detection of cyber security events.

b) Procedures and processes for detecting cyber security events from recorded events.

c) Rules, procedures and processes for evaluating and responding to detected cyber security events, including escalation procedures and contacts to relevant persons.

d) Rules and procedures for optimizing the settings of tools designed for the detection of cyber security events.

e) Rules and procedures for optimally setting the security features of the tool for collecting and evaluating cyber security events.

f) Measures to protect access to records of these events.

1.19. Vulnerability management policy and patch management

a) Rules and procedures for restricting the installation of software.

b) Rules and procedures for ensuring the support of technical assets.

c) Rules and procedures for registration of unsupported technical assets by the manufacturer, supplier or other person.

d) Rules and procedures for working with updates, patches and new versions of program resources and equipment and how to search for them.

e) Rules and procedures for testing updates, patches and new versions of software resources and equipment.

f) Rules and procedures for deployment of updates, patches and new versions of program resources and equipment, including procedures and processes for any unhurried deployment and restoration of the original state (rollback).

g) Rules and procedures for scanning vulnerabilities, working with findings and subsequent retesting of findings.

h) Rules and procedures for penetration testing, working with findings and subsequent retesting of findings.

1.20. Cryptography Use Policy

a) Rules and procedures for the use of cryptographic algorithms especially in software and equipment and within the communication network.

b) Rules and procedures for regular updating of cryptographic algorithms, especially based on issued recommendations, methodologies and security standards.

c) Rules and procedures for managing cryptographic keys and certificates.

d) Rules and procedures for securing voice, audiovisual, text (including e-mail) communication and emergency communication within the organization.

e) Rules and procedures for encryption and integrity control of information and data.

f) Rules and procedures for encryption of technical assets that are carriers of information and data (especially removable devices, disks, backup media).

1.21. Long-term storage, backup and recovery policy

a) Backup, recovery and backup retention requirements.

b) Rules and procedures for long-term storage of information and data.

c) Rules and procedures for engaging and removing a technical asset within the backup system.

d) Backup rules and procedures.

e) Backup recovery rules and procedures.

f) Rules and procedures for checking the usability of backups made.

g) Rules, procedures and periodicity for testing backups and restores.

h) Policy and rules for access to backups and stored information and data.

2. Content of safety documentation

2.1. Cybersecurity audit execution plan.

2.2. Cyber Security Audit Report

a) Cyber Security Audit Objectives.

b) The subject of a cyber security audit.

c) Cyber Security Audit Criteria.

d) Identifying the team of auditors and individuals who participated in the cyber security audit.

e) The date and location where the cybersecurity audit activities were performed.

f) Cyber Security Audit Findings.

g) Cyber security audit findings.

h) Corrective actions to ensure compliance with cybersecurity audit criteria.

2.3. Information Security Management System Review Report

a) Evaluation of the security measures from the previous review of the information security management system.

b) Identification of changes and circumstances that may affect the information security management system.

c) Feedback on the effectiveness of information security management

1) disagreements and corrective actions,

2) monitoring and measurement results,

3) audit results,

4) fulfillment of the objectives of the information security management system.

d) Assessing the results of the risk assessment and the status of the risk management plan.

e) Assessing the impact of cyber security incidents on the services provided and cyber security.

f) Assessment of changes that may have a negative impact on the information security management system.

g) Identifying opportunities for continuous improvement.

h) Recommending the necessary decisions, establishing security measures and persons ensuring the performance of individual activities.

2.4. Methodology for identifying and evaluating assets

a) Determination of the scale for the assessment of primary assets

1) determination of a scale for assessing asset confidentiality levels,

2) determination of a scale for assessing asset integrity levels,

3) determining a scale for assessing asset availability levels.

b) Determining a scale for evaluating supporting assets, taking into account the linkages between assets.

2.5. Methodology for risk identification and assessment

a) Determination of risk assessment scale

1) determination of the scale for assessing the value of the asset,

2) determination of a scale for evaluating threat levels,

3) determination of a scale for evaluating levels of vulnerability,

4) determining a scale for assessing risk levels.

b) Methods and approaches for risk management.

c) Ways of approving acceptable risks.

2.6. Asset and Risk Assessment Report

a) Summary of the asset and risk assessment process.

2.7. Statement of Applicability

a) An overview of the security measures required by this decree that were not applied, including the reasons why they were not applied.

b) An overview of applied security measures, including the method of their implementation.

2.8. Risk management plan

a) Goals and benefits of selected security measures for managing individual risks, including links to specific risks.

b) Resources needed for individual security measures for risk management.

c) Persons ensuring the enforcement of individual security measures for risk management.

d) Dates for the introduction of individual security measures for risk management.

e) Method of implementation of security measures.

2.9. Security awareness development plan

a) Content and timing of training for users, administrators, security role holders, suppliers and senior management.

b) Content and dates of initial and regular training.

c) Overviews that contain the subject of individual trainings and a list of people who completed the training.

d) Forms and methods of evaluating the effectiveness of the security awareness development plan.

2.10. Overview of generally binding legal regulations, internal regulations and other

regulations and contractual obligations

a) Overview of generally binding legal regulations.

b) Overview of internal regulations and other regulations.

c) Overview of contractual obligations.

2.11. Methodology for carrying out impact analysis

a) Ways of assessing the impact of cyber security incidents on continuity and assessing related risks.

2.12. Business continuity plans

a) Plan activation conditions.

b) Specification of persons to follow the plan.

c) Temporary solutions and procedures to ensure service continuity in the event of a crisis scenario.

2.13. Recovery plans

a) Detailed procedures for data recovery including sequence of activities, responsible persons, required time and resources.

b) How to verify successful data recovery from backup.

c) Location and description of backups.

2.14. Records of technical assets that are no longer supported by the manufacturer, supplier or other person

a) A description of these technical assets.

b) The guarantors of these technical assets.

c) Ways of introducing security measures that guarantee a similar or higher level of security of these technical assets.

2.15. Records of technical assets, accounts and authentication mechanisms that do not meet the requirement for multi-factor authentication

a) A description of these technical assets, accounts and authentication mechanisms

b) Reasons for not implementing multi-factor authentication

2.16. Other recommended documentation

a) Infrastructure topology.

b) Infrastructure segmentation.

c) An overview of technical assets within the scope of the information security management system, in particular network devices, active elements, end devices and servers,

d) Connection to contact persons who are entrusted with the performance of system and technical support.

Annex No. 6 to Decree No. XXXX Coll.

Committee on Cyber Security Management and Security Roles

This appendix contains a description of the recommended requirements for the Cyber Security Management Committee and the security roles referred to in Sections 5 and 6.

Tab. No. 1: Cybersecurity Governance Committee

Role:	Cyber Security Governance Committee
Key activities:	a) Responsibility for the overall management and development of cyber security within the obliged entity. b) Creation of the cyber security framework, direction and principles of cyber security of the obliged entity (definition of strategic goals and direction of development in the field of cyber security). c) Definition of roles and responsibilities within the information security management system. d) Definition of information security management system reporting and review requirements. e) Checking the current state of cyber security within the obliged entity and ascertaining whether the planned goals are being met.
Other conditions:	a) A member of the cyber security management committee must be at least 1. a representative of top management or a person authorized by him, 2. Cyber Security Manager. b) The members of the cyber security management committee meet regularly, while the proceedings and outputs of the meetings are kept in paper or electronic form.

Tab. #2: Cyber Security Manager

Role:	Cyber Security Manager
Key activities:	a) Responsibility for managing the information security management system. b) Regular reporting for the top management of the liable entity. c) Regular communication with the top management of the liable entity. d) Coordination and participation in the asset and risk management process. e) Submission of asset and risk assessment reports, risk management plan and statement of applicability to the Cyber Security Management Committee. f) Providing guidelines for ensuring information security in the creation, evaluation, selection, management and termination of supplier relationships. g) Communication with Government or National CERT. h) Coordination of incident management. i) Evaluating the appropriateness and effectiveness of security measures.
Knowledge:	a) Standards of the ISO/IEC 27000 series and similar standards in the field of security and ICT. b) Overview of ICT (operating systems, databases, applications, data networks) with an emphasis on security c) Risk management. d) Business continuity management. e) Relevant legal and regulatory requirements, especially the law. f) Context of the obliged person.
Experiences:	a) Enforcement of the information security management system. b) Understanding risk definitions and risk scenarios. c) Risk management within the obliged entity. d) Ability to interpret risk management results and coordinate risk management.
Education and experience:	a) At least 3 years of experience in the field of information or cyber security, or b) graduation from university and at least 1 year of experience in the field of information or cyber security.
Relevant certification	Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional

*:	(CISSP), BI Manager (CIA accreditation scheme).
Other conditions:	a) The role is not compatible with the roles responsible for the operation of the information and communication system and with other operational or management roles. b) For the proper performance of this role, it is necessary to ensure the necessary powers, responsibilities and budget.

Tab. #3: Cyber Security Architect

Role:	Cyber Security Architect
Key activities:	a) Responsibility for the design of the implementation of security measures. b) Responsibility for establishing, documenting, maintaining and continuously developing the appropriate secure architecture of the regulated service according to current good practice
Knowledge:	a) Architecture of information and communication systems and its design. b) Hardware components, tools and architectures. c) Operating systems and software. d) Business processes and their integration and dependence on ICT. e) Safety and risk management. f) Security of communications and networks. g) Management of identities and accesses. h) Safety evaluation and testing. i) Traffic safety. j) Basic principles of secure software development. k) Integration and dependencies of ICT and business processes.
Experiences:	a) Designing the implementation of security measures. b) Designing a security architecture with a focus on goals and security. c) Security of software development.
Education and experience:	a) At least 3 years of experience in the field of information or cyber security, or b) graduation from university and at least 1 year of experience in the field of information or cyber security.
Relevant certification *:	Certified Ethical Hacker (CEH), CompTIA Security +, Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), BI Manager (CIA accreditation scheme).
Other conditions:	The role is not compatible with roles responsible for the operation of information and communication systems.

Tab. 4: Cyber Security Auditor

Role:	Cyber Security Auditor
Key activities:	a) Conducting a cyber security audit. b) Evaluation of the correctness and effectiveness of the established security measures.
Knowledge:	a) Information security audit methodology and framework. b) Internal audit processes and procedures. c) Role and function of internal audit. d) The process of conducting an ICT security audit. e) Strategic and tactical management of ICT. f) Acquisition, development and deployment of ICT.

	g) Management of operation, maintenance and ICT services. h) Protection of assets. i) Cyber security assessment, testing and sampling methods. j) Relevant legal regulations. k) ICT security.
Experiences:	a) Planning information or cyber security audits. b) Conducting cyber security audits or information security management system audits. c) Analyzing the results of audits. d) Writing audit conclusions, their presentation and proposing recommendations leading to the correction of findings. e) Reporting on the status of compliance with legal requirements. f) Conducting audits with a focus on ICT and information or cyber security.
Education and experience:	a) At least 3 years of experience in information or cyber security auditing, or b) completion of studies at a university and at least 1 year of experience in the field of information or cyber security auditing.
Relevant certification *:	Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified in Risk and Information Systems Control (CRISC), Lead Auditor Information Security Management System (Lead Auditor ISMS), BI Auditor (ČIA accreditation scheme).
Other conditions:	a) The role is not compatible with roles 1. of the cyber security management committee, 2. cyber security manager, 3. cyber security architect, 4. asset guarantor. b) The role is not compatible with roles responsible for the operation of information and communication systems.

Tab. 5: Guarantor of the asset

Role:	Asset guarantor
Key activities:	a) Responsibility for ensuring the development, use and security of the asset. b) Cooperation with other persons holding security roles. c) Carrying out the identification and evaluation of assets and risks.
Knowledge:	a) Good knowledge of the asset of which it is the guarantor. b) Good knowledge of internal security policies and methodologies (for example, Asset and Risk Assessment Methodology).

* The certification may be different from the one listed, if the certification documenting the professional competence of security roles meets the requirements of ISO 17024.

Annex No. 7 to Decree No. XXXX Coll.

management - security measures for contractual relationships

Content of the contract concluded with important suppliers:

a) provisions on information security (in terms of confidentiality, integrity and availability),

b) provisions on authorization to use data,

c) provisions on the authorship of program code, or on program licenses,

d) provisions on control and audit of the supplier (customer audit rules),

e) provisions governing the chain of suppliers, while it must be ensured that the subcontractors undertake to fully comply with the agreement between the obliged entity and the supplier and do not conflict with the requirements of the obliged entity for the supplier,

f) provisions on the supplier's obligation to comply with the security policies of the obliged entity or provisions on the approval of the supplier's security policies (or the approval for the supplier relationship of the relevant parts of the security policies) by the obliged entity,

g) change management provisions,

h) provisions on compliance of contracts with generally binding legal regulations,

i) provisions on the obligation of the supplier to inform the obliged person about

   1. cyber security incidents related to the performance of the contract,
   2. method of risk management on the part of the supplier and residual risks related to the performance of the contract,
   3. to a significant change in the control of this supplier according to the Act on Business Corporations or a change in the ownership of essential assets, or a change in the authorization to dispose of these assets, used by this supplier to perform according to the contract with the obliged entity,
   4. a request from a foreign authority to make available or hand over data processed on the territory of a foreign state, except for situations where such information would be in conflict with the legal order under which the data is processed or according to which the request was submitted.

j) specification of conditions from the point of view of security at the end of the contract, the so-called exit strategy (for example, a transitional period at the end of cooperation, when the service still needs to be maintained before the deployment of a new solution, data migration, etc.),

k) specification of conditions for business continuity management in connection with suppliers (for example, inclusion of suppliers in emergency plans, tasks of suppliers when activating business continuity management),

l) specification of the conditions for the format of the transfer of data, operational data and information upon request by the obliged entity,

m) data disposal rules,

n) provisions on the right to unilaterally withdraw from the contract in the event of a significant change in control over the supplier or a change in control over essential assets used by the supplier to perform under the contract,

o) provisions on sanctions for breach of obligations and

p) provisions on making available or handing over data based on a request from a foreign authority to make available or handing over data processed on the territory of a foreign state

   1. only after a review of the legality of the request,
   2. only after an effort has been made to prevent the disclosure or transfer of data within the scope of the possibilities given by the legal order within the scope of which the data is being processed or according to which the request was submitted,
   3. only to the extent necessary.

Annex No. 8 to Decree No. XXXX Coll.
Recommended topics for the development of security awareness

a) Device security techniques.
b) Firewall, antivirus and their limitations.
c) Malicious programs and their manifestations.
d) Risks of downloading programs and applications.
e) Software update.
f) Risks of enabling/disabling running macros.
g) Risks of Executable Files.
h) User Account Security Policy.
i) Using, creating and managing passwords.
j) Multi-factor authentication.
k) Social engineering techniques.
l) Online identity, digital footprint and its minimization.
m) Principles of work in a computer network.
n) Using a remote connection (VPN).
o) Secure electronic communication.
p) Website security.
q) Data backup, storage and encryption.
r) Safe use of portable technical data carriers.
s) Use of cloud storage.
t) Rules and procedures for reporting unusual behavior of technical assets and suspicions of any vulnerabilities.
u) The basic procedure for responding to a cyber security event or incident.
v) Policy for using work equipment for private purposes.
w) Policies for use of private devices for work purposes (BYOD security).
x) Personal responsibility of the employee in compliance with the principles of cyber security.
Current threats in cyber security.

Decree on the security measures of the regulated service provider in the regime of lower obligations

Proposal

DECREE

from dd.mm.yyyy ,

on the security measures of the provider of the regulated service in the regime of lower obligations

The National Office for Cyber and Information Security establishes pursuant to § 55 paragraph 1 letter c) and d) of Act No. [to be supplemented] Coll., on cyber security (hereinafter referred to as "the Act"):

PART ONE

INTRODUCTORY PROVISIONS

§ 1

Subject of legislation

This decree incorporates the relevant regulation of the European Union [40]and for regulated service providers in the regime of lower obligations (hereinafter referred to as the "obligated person") regulates

a) content and scope of security measures a
b) method of determining the significance of the impact of a cyber security incident.

§ 2

Definition of terms

For the purposes of this decree, it is understood

a) administrator, a privileged user or a person ensuring the management, operation, use, maintenance and security of a technical asset,
b) a security policy is a set of principles and rules that determine the way to ensure the protection of assets,
c) a privileged user is an authority or person whose activity on a technical asset may have a significant impact on the security of the regulated service,
d) the user is a natural or legal person or public authority that uses the assets,
e) top management means the person or group of persons who manage the obliged entity, or the statutory body of the obliged entity,
f) by ensuring cyber security, ensuring the minimum level of cyber security of the assets

[40] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cyber security in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 20/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive) .

of the obliged entity based on the introduction of security measures.

PART TWO

SAFETY PRECAUTIONS

§ 3

The obligated person shall introduce and implement security measures in accordance with this decree within the scope of cyber security management established pursuant to Section 13 of the Act.

§ 4

Ensuring cyber security

(1) As part of ensuring cyber security, the obliged person shall implement and implement adequate security measures taking into account the organization's security needs. The obliged person always implements and implements at least security measures according to Sections 4 to 6 and Section 11.

(2) Mandatory person

a) prepares an overview of the security measures required by this decree according to Annex No. 1, which contains at least

1. an overview of all security measures that have been implemented, including a description of their implementation,
2. an overview of all security measures that will be implemented, including the dates for their implementation, the priority of their implementation, the designation of the person responsible for their implementation and
3. an overview of all security measures that were not implemented, including the justification for not implementing them,

b) at least once a year, he conducts and documents an evaluation of the effectiveness of implemented security measures, including an update of the overview of security measures,

c) keeps individual summaries of security measures with which top management has demonstrably become familiar with pursuant to § 5 letter c) for at least 4 years.

(3) The obliged entity shall designate a person responsible for cyber security who is responsible for the management and development of cyber security, oversight of the state of cyber security and communication in the field of cyber security with senior management, and a person may be authorized for this activity

a) without unnecessary delay completes professional training in accordance with § 6 letter g) or

b) demonstrate professional competence in the field of cyber security.

(4) Mandatory person in the management of security policy and security documentation

a) creates and approves a security policy and maintains security documentation covering the areas listed in Annex No. 2 to this decree,

b) updates relevant security policies and security documentation.

(5) The obliged person complies with the rules and procedures established in the security policy and security documentation pursuant to paragraph 4 letter and).

(6) In accordance with the identification and registration of assets according to the law, the obliged person establishes and implements protection rules and permissible ways of using assets.

(7) When entering into a contract with suppliers, the obliged person shall ensure that the contracts with these suppliers include, in particular, the relevant areas listed in Annex No. 3 to this decree.

(8) In connection with the planned acquisition, development and maintenance of technical assets, the obliged person establishes security requirements in the field of cyber security and enforces their compliance, based in particular on the requirements for security measures according to this decree.

§ 5

Duties of top management

Senior management with regard to ensuring cyber security

a) is demonstrably instructed in his duties and scope of responsibilities,
b) ensure the availability of the resources needed to ensure cyber security in accordance with the overview of security measures,
c) is demonstrably familiar with the fulfillment of the overview of security measures according to § 4 paragraph 2 letter and).

§ 6

Security of human resources

Mandatory person in the framework of human resources security

a) establishes a policy for the safe behavior of users, within which it takes into account the relevant topics listed in Annex No. 4 of this decree,
b) establishes the rules for developing security awareness, including the rules for creating passwords according to § 9,
c) in accordance with the rules for the development of security awareness, conducts introductory training in the field of cyber security,
d) in accordance with the rules for the development of security awareness, conducts regular training in the field of cyber security,
e) as part of the training according to letter c) and d) takes into account the relevant topics listed in Annex No. 4 of this decree,
f) keeps overviews of trainings according to letter c) and d),
g) will ensure the necessary professional theoretical and practical training of administrators and persons responsible for cyber security in accordance with their work content,
h) ensure compliance with the security policy and
i) determine the rules and procedures for dealing with cases of violation of the established rules.

§ 7

Business continuity management

Mandatory person in the framework of business continuity management

a) within the framework of primary assets, it determines their priority and order and procedures for their renewal,
b) determines the responsibilities and obligations during the renewal according to letter and),
c) creates regular backups of technical asset settings, information and data necessary especially for the purpose of restoring the regulated service in the event of a cyber security incident.

§ 8

Access control

(1) Based on operational and security needs, the obliged person controls access to assets, within the framework of access control
   a) assign access rights and authorizations and a unique identifier to each user and administrator accessing technical assets,
   b) limit the allocation of administrative and privileged permissions to the level necessary to perform the job,
   c) manages the identifiers, access rights and authorizations of technical asset accounts,
   d) introduces the security measures necessary for the safe use of mobile devices and other technical devices, as well as security measures connected with the use of technical devices that the obligated person does not have under his control,
   e) performs a regular review of the settings of all access permissions,
   f) ensure the removal or change of access rights when changing the position or inclusion of users or administrators,
   g) ensure the removal or change of access authorizations upon termination or change of the contractual relationship and
   h) sets out the rules for creating passwords according to § 9.
(2) As part of physical security, the obliged person prevents unauthorized access to his assets and prevents their damage, theft and unauthorized interventions.

§ 9

Identity management and their authorization

(1) The obliged person uses a tool to manage identities and their authorizations
   a) management of access rights
   b) identity management,
   c) managing the number of possible failed login attempts,
   d) re-verification of identity after a specified period of inactivity a

e) durability of stored and transmitted authentication data.

(2) The obliged person to verify the identity of administrators and users uses an authentication mechanism that is based on multi-factor authentication with at least two different types of factors.

(3) Until the use of the authentication mechanism based on multi-factor authentication according to paragraph 2, the obliged person uses authentication using cryptographic keys or certificates.

(4) Until the use of the authentication mechanism using cryptographic keys or certificates according to paragraph 3, the obliged person uses a tool based on authentication using an account identifier and a password, and this tool must enforce the following rules

a) password length at least
   1. 12 characters for user accounts,
   2. 17 characters for administrator accounts,
   3. 22 characters for technical asset accounts,
b) to verify the identity of the technical assets, the default password must be changed immediately and a new password must be created with a random string composed of uppercase and lowercase letters, numbers and special characters,
c) unrestricted use of lower and upper case letters, numbers and special characters,
d) mandatory password change at an interval of no more than 18 months,
e) disallowing users and administrators
   1. choose simple and frequently used passwords,
   2. create passwords based on multiple characters, login name, email, system name or similar and
   3. reuse of previously used passwords with a memory of at least 12 previous passwords.

(5) Obliged person further within the framework of identity management

a) ensure confidentiality is maintained in the creation of default credentials and in the recovery of access a
   1. ensure the change of the default password or the password used to restore access after its first use,
   2. invalidate the password or identifier used to restore access no later than 72 hours after its creation,
b) ensure an immediate change of the access password in case of reasonable suspicion of its compromise and
c) secure administrator accounts of technical assets intended especially for recovery after a cyber security incident and use these accounts only in absolutely necessary cases.

§ 10

Detection and recording of cyber security events

(1) As part of the detection of cyber security events, the obliged person shall ensure

a) verification and control of transmitted data at the perimeter of the communication network, including blocking unwanted communication,
b) a tool for continuous and automatic protection against malicious code on

individual relevant technical assets, in particular on

1. servers,
2. end stations,

c) regular updating of detection tools and their rules,
d) control of automatic launch of content and
e) continuous provision of information on relevant detected cyber security events and timely warning of relevant persons .

(2) The obliged person records cyber security events and relevant operational events in accordance with paragraph 1 and in these events records in particular the following
a) date and time including time zone specification,
b) type of activity,
c) unambiguous identification of the technical asset and account identification a
d) success or failure of the activity.

§ 11

Resolving cyber security incidents

(1) Mandatory person in the framework of solving cyber security events and incidents
a) ensure that users, administrators, persons responsible for cyber security, other employees and suppliers report unusual behavior of technical assets and suspicions of any vulnerabilities,
b) create a methodology for assessing cyber security events and cyber security incidents, including those with a significant impact in accordance with § 15,
c) ensure the assessment of cyber security events and cyber security incidents, including those with a significant impact in accordance with the methodology under letter b),
d) ensure the resolution of cyber security incidents,
e) reports cyber security incidents with a significant impact according to § 16 of the Act,
f) creates a final report on a cyber security incident with a significant impact according to § 17 of the Act, including a description of the cause of the cyber security incident with a significant impact, if known.

(2) The obliged person shall ensure the detection of cyber security events and shall also use the tools according to § 10 during their detection.

§ 12

Security of communication networks

Mandatory person for the protection of the security of the communication network, especially its network perimeter
a) will ensure the segmentation of the communication network, in particular the separation of the operational and backup environment,
b) will limit outgoing and incoming communication on the perimeter of the communication network to what is necessary to properly ensure the provision of the regulated service,

c) uses current durable and secure network protocols,
d) in the case of using a remote connection to the internal communication network or remote management of the technical assets of the regulated service
    1. will limit these connections to those strictly necessary,
    2. implement security measures to ensure the confidentiality and integrity of such remote connections and remote administration and
    3. has an overview of users and administrators who use these remote connections or remote management.

§ 13

Application security

Mandatory person for ensuring the safety of the regulated service

a) ensure the immediate application of security updates issued for technical assets,
b) for technical assets that are no longer supported by the manufacturer, supplier or other person
    1. keeps their records,
    2. implements security measures that guarantee a similar or higher level of security and
    3. will limit their communication in the communication network to what is absolutely necessary,
c) conducts vulnerability scans of relevant technical assets and applies appropriate security measures based on the findings.

§ 14

Cryptographic algorithms

(1) Mandatory person for ensuring the protection of technical assets and their communication
    a) uses encryption using currently strong cryptographic algorithms where appropriate,
    b) promotes safe handling of cryptographic algorithms and
    c) takes into account recommendations and methodologies in the field of cryptographic algorithms issued by the Office, published on its website.
(2) The obliged person ensures a safe
    a) voice, audiovisual and text communication, including e-mail communication and
    b) emergency communication within the organization.

PART THREE

HOW TO DETERMINE THE SIGNIFICANCE OF A CYBER SECURITY INCIDENT

§ 15

Determining the significance of the impact of a cyber security incident

(1) For the purposes of evaluating the significance of the impact of a cyber security incident on the provision of a regulated service, the obligated person shall determine
   a) the life or health of persons or the ability of the regulated service provider to meet its obligations are not yet threatened,
   b) areas for assessing the significance of the impact of cyber security incidents on the organization taking into account
      1. the operational impact of a cyber security incident on the obliged entity and its ability to provide a regulated service,
      2. the number of employees, users of the regulated service and other bodies and persons affected by a cyber security incident,
      3. the time and resources required to restore the provision of the affected regulated service,
      4. the location of the incident defining the significance of part of the assets affected by a cyber security incident for the provision of a regulated service,
      5. the sensitivity of the data affected by a cyber security incident and the damage or non-pecuniary damage that a breach of the security of this data may cause to the liable person or other body or person,
      6. the cause of the cyber security incident, if it is known to the liable person, and in particular whether the direct cause was human error, a technical defect, or intent.

(2) The impact of a cyber security incident on the provision of a regulated service is considered significant if it exceeds the tolerable level of damage caused by a cyber security incident as determined by the obliged entity pursuant to paragraph 1 letter a), and at the same time, based on the areas according to paragraph 1 letter b) assessed as significant.

PART FOUR

EFFECTIVENESS

§ 16

Effectiveness

This decree becomes effective on dd.mm.yyyy .

Director:
Ing. Lukáš Kintr incl

-

Annex No. 1 to Decree No. XX/XXXX Coll.

Overview of security measures

Evaluation of the effectiveness of ensuring cyber security for the given year					
Safety measures required by decree	Security measure status (implemented / not implemented/ in the process of being implemented)	Description of the security measure/ justification for not implementing the security measure	Planned date of introduction of the security measure	The priority of implementing a security measure	The person responsible for implementing the security measure

Annex No. 2 to Decree No. XX/XXXX Coll.
Security policy and security documentation

1. Policy for ensuring a minimum level of cyber security
    a) The scope and boundaries of cyber security management.
    b) Protection rules and permissible uses of assets.
    c) Requirements of the service level agreement and the method and level of implementation of security measures.
    d) Security requirements for acquisition, development and maintenance management.

2. Human resource security policy
    a) Rules for the development of security awareness and records of training overviews.
    b) Safety training for new employees.
    c) Establishing a period for regular training.
    d) Rules for handling security policy violations.
    e) Rules for termination of employment or change of job position
        I. return of entrusted assets and withdrawal of rights upon termination of the employment relationship,
        II. change of access rights when changing job position,
        III. transfer of responsibilities upon change of job position or termination of employment with administrators or the person responsible for cyber security .
    f) Rules of safe behavior of users, including rules for creating passwords.

3. Business Continuity Management Policy
    a) Prioritization of primary assets and the order and procedures of their renewal, including the determination of responsibilities.
    b) Communication matrix with key persons for individual services.
    c) Procedures for starting and stopping the system, for restarting or resuming the system after a failure, and for handling error conditions or extraordinary phenomena.
    d) Backup rules and procedures.

4. Access control policy
    a) Rules and procedures for managing privileged access.
    b) Rules, procedures and records for accounts used especially for recovery after a cyber security incident.
    c) Rules for regular review of access rights, including the division of individual users into access groups.

5. Cyber Security Event Detection and Cyber Security Incident Resolution Policy
    a) Defining a cyber security event and a cyber security incident.
    b) Rules and procedures for the identification and classification of incidents with a significant impact according to part three of this decree.
    c) Rules and procedures for reporting unusual behavior of technical assets and suspicions of any vulnerabilities.
    d) Reporting of high-impact cyber security incidents.

6. Communication network security policy
    a) Rules and procedures for controlling remote access to the communications network, including remote access by vendors or others.
    b) Rules and procedures for remote management of technical assets, including remote management of technical assets by a supplier or other persons.

7. Application Security Policy
    a) Rules for regular updates.
    b) Rules for securing technical assets that are no longer supported.
    c) Rules for scanning vulnerabilities.

8. Asset records

9. Overview of security measures

10. Recovery plans

11. Final Cyber Security Incident Report

12. Records of unsupported technical assets

13. Other recommended documentation
    a) Infrastructure topology.
    b) Infrastructure segmentation.
    c) Overview of technical assets, especially network devices, active elements, end

devices and servers.

d) Contacts for persons in charge of technical and system support.

Annex No. 3 to Decree No. XX/XXXX Coll.
Requirements for contractual arrangements with suppliers

The content of the contract concluded with suppliers determines the methods of implementation of security measures and determines the content of mutual contractual responsibility for the introduction and control of security measures .

Content of the contract with suppliers:

a) provisions ensuring information security (requirement to ensure confidentiality, integrity and availability) ,
b) supplier audit provisions ,
c) provisions on chaining of suppliers ,
d) provisions regulating the so-called exit strategy, conditions for terminating the contractual relationship from the point of view of security,
e) provisions on sanctions for breach of contractual obligations,
f) provisions on authorization to use data,
g) provisions on the authorship of program code, or on program licenses ,
h) provisions on the confidentiality of the contractual relationship,
i) provisions regulating the obligation to comply with the rules for suppliers, with which the relevant employees of the supplier have been demonstrably familiarized,
j) change management provisions,
k) provisions on cyber security incidents related to the performance of the contract,
l) provisions governing the provision of business continuity management,
m) details of the service level agreement (SLA) and the method and level of implementation of security measures .

When concluding contracts with suppliers, the obliged person is recommended to request other arrangements taking into account specific requirements arising from the provision of operational and security needs related to the regulated service not listed in this appendix.

Annex No. 4 to Decree No. XX/XXXX Coll.
Recommended topics for the development of security awareness

a) Device security techniques
b) Firewall, antivirus and their limitations
c) Malicious programs and their manifestations
d) Risks of downloading programs and applications
e) Software update
f) Risks of enabling/disabling running macros

g) Risks of Executable Files
h) User Account Security Policy
i) Using, creating and managing passwords
j) Multi-factor authentication
k) Social engineering techniques
l) Online identity, digital footprint and its minimization
m) Principles of work in a computer network
n) Using a remote connection (VPN)
o) Secure electronic communication
p) Website security
q) Data backup, storage and encryption
r) Safe use of portable technical data carriers
s) Use of cloud storage
t) Rules and procedures for reporting unusual behavior of technical assets and suspicions of any vulnerabilities
u) The basic procedure for responding to a cyber security event or incident
v) Policy for using work equipment for private purposes
w) Policy for use of private devices for work purposes (BYOD security)
x) Personal responsibility of the employee in compliance with the principles of cyber security
y) Current threats in cyber security

Decree on the NÚKIB Portal and requirements for selected actions

Proposal

DECREE

from dd.mm.yyyy ,

about the NÚKIB Portal and requirements for selected actions

The National Office for Cyber and Information Security establishes pursuant to § 55 paragraph 1 letter e), i) and j) of Act No. [*to be added*], on cyber security (hereinafter referred to as "the Act"):

§ 1

NÚKIB portal

(1) Access to the NÚKIB Portal and its subsequent use is carried out via the Office's website after logging in using the assigned login data.
(2) Within the NÚKIB Portal, the Office will make available forms for
   a) registration of a regulated service provider according to § 8 of the Act,
   b) changing the registration of the regulated service provider according to § 9 of the Act,
   c) data reporting according to § 12 of the Act,
   d) reporting of incidents according to § 16 and 17 of the Act,
   e) notification of implementation of countermeasures according to § 20, paragraph 3 of the Act,
   f) reporting information about suppliers according to § 32 of the Act, and
   g) reporting the implementation of corrective measures according to § 57 of the Act.

§ 2

Types of reported data

(1) Registration data is understood
   a) identification data of the provider of the regulated service, which are its name, identification number, address of the registered office, and possibly the main establishment and other establishments in other member states of the European Union,
   b) the list of provided regulated services fulfilling the criteria for identifying regulated services and the criteria fulfilled by the provider of the regulated service according to the decree on regulated services,
(2) Contact data means the first and last name and, where applicable, other data enabling the unambiguous identification of the authorized or authorized person, their role or job position vis-à-vis the provider of the regulated service, their telephone number and e - mail address .
(3) Additional data means domain names, autonomous system numbers (ASN) and IP address ranges that are used to provide the regulated service, if any, information on the geographical distribution of the regulated service, its cross-border provision and the ownership structure of the provider of the regulated service.

§ 3

Reporting a cyber security incident

(1) The form for reporting a cyber security incident by a regulated service provider contains
   a) identification data of the provider of the regulated service, including a list of the regulated services provided by him,
   b) contact information,
   c) additional data on affected systems and services,
   d) information about the cyber security incident , in particular the date and time of detection, the status of the incident, the probable cause of the incident, description of the incident, indicators of compromise, if this information is available,
   e) information defining the impact of the incident, in particular the functional impact, an estimate of the extent and number of affected systems, machines, assets or people, the time and resources required to restore the provision of the affected service, the location of the incident and the sensitivity of the affected data, and any cross-border impact of the incident, if this information is available ,
   f) information on the response to a cyber security incident, in particular the required support from the Office, the measures taken and ongoing to mitigate the consequences and the entities that were informed in connection with the incident.

(2) Through the cyber security incident reporting form, the regulated service provider can make
   a) initial report according to § 17 paragraph 1 of the Act,
   b) notification of an incident according to § 17 paragraph 3 letter a) of the law,
   c) submission of an ongoing report on significant changes in the state of cyber security incident management pursuant to § 17 paragraph 3 letter b) of the Act,
   d) submission of the final report pursuant to § 17 paragraph 3 letter c) of the law,
   e) submission of an ongoing report on the current status of managing a cyber security incident pursuant to § 17 paragraph 3 letter c) of the Act.

(3) If the provider of the regulated service reports a cyber security incident in accordance with § 16 of the Act other than through the NÚKIB Portal, the content requirements according to paragraph 1 shall apply accordingly.

(4) If a cyber security incident is reported via the Office's website by a voluntary whistleblower in accordance with § 16 paragraph 5 of the Act, which is not a regulated service provider, contains a form
   a) identification and contact details of the notifier or other contact person,
   b) identification and description of the information system or service affected by the cyber security incident,
   c) information about the cyber security incident, in particular the date and time of detection, the type of threat or the root cause that probably triggered the incident, an estimate of the extent of affected systems, an estimate of the number of affected users, a detailed description of the incident and any cross-border impact of the incident, if this information is available,
   d) information on the response to a cyber security incident, in particular the status of incident management, measures taken and ongoing to mitigate the consequences.

§ 4

Content requirements of selected acts

(1) The form for registering a regulated service provider and for changing this registration contains registration data.

(2) The data reporting form contains
   a) identification data of the provider of the regulated service, including a list of the regulated services provided by him,
   b) contact information,
   c) Additional Information.

(3) The form for reporting the implementation of countermeasures contains
   a) identification data of the provider of the regulated service, including a list of the regulated services provided by him,
   b) contact information,
   c) additional data relevant with regard to the content of countermeasures,
   d) identification of countermeasures,
   e) information about the execution of the countermeasure and its result.

(4) The supplier information reporting form contains
   a) identification data of the provider of the regulated service,
   b) identification data of the supplier of safety-relevant supplies ,
   c) identification of safety-relevant supplies,
   d) identification of the critical part of the range,
   e) identification of the regulated service to which the safety-relevant delivery is linked ,
   f) information about the direct or indirect relationship with the supplier.

(5) The corrective action report form contains
   a) identification data of the provider of the regulated service, including a list of the regulated services provided by him,
   b) contact information,
   c) additional data relevant with regard to the content of the corrective measure,
   d) identification of corrective action,
   e) information about the implementation of the corrective measure and its result.

§ 5

Data reporting by an entity providing domain name registration services

Data pursuant to § 35 of the Act are reported via a form published on the website of the Office.

§ 6

Format and structure of actions

Actions according to § 44, paragraph 2 of the Act must be delivered to the Office in an open and machine-readable format.

§ 7

Effectiveness

This decree becomes effective on dd.mm.yyyy .

Director:
Ing. Lukáš Kintr incl

Decree on inalienable functions of a specified scope

Proposal

DECREE

from dd.mm.yyyy ,

on indispensable functions of the specified scope

The National Office for Cyber and Information Security establishes pursuant to § 55 paragraph 1 letter g) Act No. [to be added] Coll., on cyber security (hereinafter referred to as "the Act"):

§ 1

Subject of legislation

This decree regulates essential functions of the specified scope for the regulated service of providing a public communication network and the regulated service of providing a publicly available electronic communications service according to the annex to Decree No. [to be added] Coll., on regulated services.

§ 2

Definition of terms

For the purposes of this decree, public communication network means a public communication network according to the legal regulation governing electronic communications [41].

§ 3

Indispensable functions

Indispensable functions according to § 28, paragraph 4 of the Act are listed in the annex to this decree.

§ 4

Effectiveness

This decree becomes effective on dd.mm.yyyy .

Director:
Ing. Lukáš Kintr incl

Annex to Decree No. [to be added] Coll.

[41] § 2 paragraph 2 letter d) Act No. 127/2005 Coll., on electronic communications and on the amendment of some related laws (Electronic Communications Act), as amended.

Essential features

Category of indispensable functions		Description of an indispensable function
1. Essential functions in a public communications network related to the management of network resources, routing and other control or management of end-user traffic in a public communications network that may have a significant impact on network traffic	1.1	Logging, managing access, authenticating and authorizing end users, allocating network resources to end users, and managing end user connections and sessions.
	1.2	Registration, authentication and authorization of public communication network functions and network services.
	1.3	A function enabling access to data on the geographic location of terminal devices processed within the public communication network or enabling the determination of the location of the device using the means of the public communication network.
	1.4	Functions related to the storage of network and end-user data.
	1.5	Infrastructure services necessary to support the operation of the public communications network and publicly available electronic communications services.
	1.6	A feature that introduces an interface for connecting between individual public communication networks or services, including roaming.
	1.7	Features related to exposing the network core to external applications.
	1.8	Functions by which public communication networks or services are interconnected, if such function may have a significant impact on access to the public communication network or on network traffic.
	1.9	Centralized management of public communications network encryption, public communications network functions, and end-user traffic and encryption keys.
	1.10	Security functions of information affecting the essential functions of the public communication network.
	1.11	Public communication network management and monitoring systems, including cyber security management and monitoring, if these systems relate to the management or monitoring of essential functions of the public communication network, or if they may have a significant impact on network access or network traffic.
	1.12	Billing, support and back -end systems that may have an immediate significant impact on access to the public communications network or network traffic.
	1.13	A feature that introduces the recording and monitoring of operational and location data.
	1.14	2nd, 4th and 5th generation radio access network management functions and base station

		management.
	1.15	A virtualization function, when used to implement an essential function or measure considered to be an essential function of a public communications network, and any function or measure falling under such virtualization.
2. Essential functions of 4th generation networks - public communication network operated using the 3GPP LTE standard (Release 8 and higher) or the IEEE 802.16m standard	2.1	A subscriber registry that stores data for processing user connections and sessions [Home Subscriber Server (HSS)].
	2.2	A gateway providing a connection between a user device and an external packet data network [Packet Gateway (PGW)].
	2.3	A gateway connecting packets between the operator's internal IP network and the external IP network [Packet Data Network Gateway (PDN GW)].
	2.4	A gateway used to establish connections between users with access outside of 3GPP traffic routing [Evolved Packet Data Gateway (ePDG)].
	2.5	Features used to manage user connection policies and charging [Policy and Charging Rules Function (PCRF)].
	2.6	Function responsible for end-to-end connectivity and mobility management [Mobile Management Entity (MME)].
	2.7	The gateway responsible for routing user-level traffic [Serving Gateway (SGW)].
	2.8	Function forwarding name of the central database containing user data of the HSS function from the subscriber register to other network functions [Subscription Locator Function (SLF)].
	2.9	Equipment Identity Register containing information about the authorization to use the mobile device [Equipment Identity Register (EIR)].
	2.10	The server responsible for authentication and authorization of users with access outside the 3GPP network [3GPP AAA Server].
	2.11	Proxy server responsible for authenticating and authorizing users with access outside the 3GPP network [3GPP AAA Proxy Server].
	2.12	A function that controls user traffic between the mobile network and access networks outside the 3GPP network [Access Network Discovery and Selection Function (ANDSF)].
3. Indispensable functions of 5th generation networks - a public communication network complying with the standard of electronic communications networks according to the 3GPP/ETSI specification	3.1	User terminal authentication function [Authentication Server Function (AUSF)].
	3.2	The function responsible for termination of operation in the control plane, registration of end devices and mobility management [Access and Mobility Management Function (AMF)].
	3.3	Functions for storing and retrieving unstructured data [Unstructured Data Storage Function (UDSF)].

including at least the 5G NR (New Radio) access radio network standard in an architecture that meets the requirements of the ETSI TS 123 501 (3GPP TS 23.501) and ETSI specifications TS 138 401 (3GPP TS 38.401) or more current.	3.4	A feature that enables the provision of core 5G networking functionality to third parties and external applications [Network Exposure Function (NEF)].
	3.5	A feature that allows the core functionality of 5th generation networks to be provided to third parties and external applications [Intermediate Network Exposure Function (I-NEF)].
	3.6	Network service availability control, registration and authorization functions [Network Repository Function (NRF)].
	3.7	The function responsible for network segmentation services and specifications [Network Slice Selection Function (NSSF)].
	3.8	Function responsible for authentication and authorization of individual network segments [Network Slice Specific Authentication and Authorization Function (NSSAAF)].
	3.9	Function responsible for traffic control and implementation of access control policy [Policy Control Function (PCF)].
	3.10	User session management function [Session Management Function (SMF)].
	3.11	Functions controlling user access and creation and management of encryption keys [Unified Data Management (UDM)].
	3.12	A data repository capable of storing and retrieving information (especially subscriber information) [Unified Data Repository (UDR)].
	3.13	Function responsible for routing, control and control of traffic on the user data plane [User Plane Function (UPF)].
	3.14	Functions for saving and storing identification data of user devices (so-called radio capability ID data) [UE Radio Capability Management Function (UCMF)].
	3.15	Functions supporting network routing decisions [Application Function (AF)].
	3.16	Device or equipment identity register that contains information about authorization to use mobile devices [5G-Equipment Identity Register (5G-EIR)].
	3.17	Functions collecting and analyzing data for network management [Network Data Analytics Function (NWDAF)].
	3.18	Functions enabling online and offline payments, which determine in particular the billing of the user for the services used [Charging Function (CHF)].
	3.19	Routing messages to other network functions [Service Communication Proxy (SCP)].
	3.20	A proxy server that ensures connection with other networks [Security Edge Protection Proxy (SEPP)].
	3.21	Features enabling access to network functionalities for users outside the mobile network [Non-3GPP

		InterWorking Function (N3IWF)].
	3.22	A feature that allows user equipment to connect to the core of 5th generation networks via a non-3GPP access technology [Trusted Non-3GPP Gateway Function (TNGF)].
	3.23	A function ensuring the connection between the cable network and the core of the 5th generation networks [Wireline Access Gateway Function (W -AGF)].

Decree on supplier risk criteria

Proposal

DECREE

from dd.mm.yyyy ,

about the supplier's riskiness criteria and the method of their evaluation

The National Office for Cyber and Information Security establishes pursuant to § 55 paragraph 1 letter h) Act No. [to be supplemented] Coll., on cyber security, (hereinafter referred to as "the Act"):

§ 1

Subject of legislation

This decree regulates the supplier's riskiness criteria and the method of their evaluation.

§ 2

Countries influencing the supplier

For the purposes of this decree, the country having influence on the supplier is understood

a) the supplier's country of residence,

b) the country in which negotiations are mainly conducted in relation to the management of the supplier or in which the management of the supplier regularly meets,

c) the country of residence of the real owner of the supplier in the sense of the legal regulation governing the registration of real owners [42],

d) the country in which the person controlling the supplier has its seat or residence in the sense of the legal regulation governing business corporations [43], or the country from which the supplier is mainly controlled, or

e) a country that can arbitrarily, directly or indirectly, effectively exert pressure on the supplier, influence it in a decisively significant way or exercise decisive influence in the sense of the legal regulation governing business corporations [44].

§ 3

Supplier risk criteria

Supplier riskiness criteria according to § 28, paragraph 4 of the Act are listed in the annex to this decree.

[42]Act No. 37/2021 Coll., on the registration of beneficial owners, as amended.

[43]Act No. 90/2012 Coll., on commercial companies and cooperatives (Act on Commercial Corporations), as amended .

[44]Act No. 90/2012 Coll., on commercial companies and cooperatives (Act on Commercial Corporations), as amended .

§ 4

Method of evaluating the supplier's riskiness criteria

In order to evaluate the supplier's riskiness criteria according to § 28, paragraph 4 of the Act , the value of the supplier's riskiness is determined according to the findings on the fulfillment of individual criteria by the supplier , which determines a possible cyber threat associated with the supplier or a possible threat to the security of the Czech Republic or internal or public order. The relevance of individual criteria for the resulting value of the supplier's riskiness is assessed according to the degree of fulfillment of individual criteria in relation to the degree of fulfillment of other criteria and other information and data collected and evaluated according to § 28, paragraph 1 of the Act .

§ 5

Effectiveness

This decree becomes effective on dd.mm.yyyy .

Director:
Ing. Lukáš Kintr incl

Annex to Decree No. [to be added] Coll.
Supplier risk criteria

Criterion number	Criterion description
1.	There is no democratic political system in the country with influence over suppliers.
2.	In a supplier-influenced country, there is no separation of powers between the legislative, executive and judicial branches.
3.	In a country with influence over suppliers, state power is not exercised solely by law, and there is no independent judicial review of the exercise of public power in the country.
4.	The legislation of the country affecting the supplier imposes an obligation to cooperate with public authorities carrying out activities corresponding to the activities of intelligence services, without independent judicial oversight or review.
5.	A country with influence over suppliers effectively enforces cooperation with public authorities that carry out activities similar to those of intelligence services, and there is no independent judicial review in the country.
6.	A country with influence over suppliers focuses its cyber strategy or doctrine on offensive operations in cyberspace against the Czech Republic or other member states of the European Union, the European Economic Area, the North Atlantic Alliance or the Organization for Economic Cooperation and Development.
7.	Countries that have influence on suppliers actively work against the interests of the Czech Republic or other member states of the European Union, the European Economic Area, the North Atlantic Alliance or the Organization for Economic Cooperation and Development.
8.	International sanctions have been imposed on the country having influence on the supplier, or there is a high probability that these international sanctions will be

	imposed on the country in question.
9.	The supplier or person who is a. by a statutory body or a member of a statutory body, or another person in a leading position within a legal entity who is authorized to act on behalf of or on behalf of the legal entity, b. in a leading position within a legal entity, who performs management or control activities for this legal entity, even if he is not a person mentioned in letter a), c. by those who exercise decisive influence on the management of this legal entity, or d. an employee of the supplier or a person in a similar position during the performance of work tasks, even if he is not a person listed in letters a) to c), she was legally convicted of a crime.
10.	There is a reasonable concern that the activities of the supplier may threaten the important economic interests of the Czech Republic.
11.	There is reasonable concern that the supplier's ability to provide performance may be significantly limited or otherwise impaired.
12.	International sanctions were imposed on the supplier in accordance with Act No. 69/2006 Coll., on the implementation of international sanctions, as amended.
13.	The supplier voluntarily cooperates with public authorities that carry out activities corresponding to the activities of the intelligence services of a country having influence on him, without being bound by the legislation of such a country, while this cooperation acts or may act against the interests of the Czech Republic.