Proposal

DECREE

dated dd.mm.yyyy,

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

The National Office for Cyber and Information Security shall determine pursuant to § 55(1)(c) of Act No. [to be added] Coll., on Cybersecurity (hereinafter referred to as "the Act"):

PART ONE
INTRODUCTORY PROVISIONS

§ 1
Subject matter of the legislation

This Decree incorporates the relevant European Union regulation[1] and for providers of a regulated service in the regime of higher obligations (hereinafter referred to as the "obliged entity") it establishes

a) the content and scope of the security measures; and
b) information and data subject to the obligation of the obliged entity to ensure their processing in the defined territory and those defined territories.

§ 2
Definition of terms

For the purposes of this Decree, the terms below are understood to have the following meanings:

a) administrator is a privileged user or person responsible for the administration, operation, use, maintenance and security of a technical asset,
b) acceptable risk is a risk that is acceptable to the obliged entity,
c) security policy is a set of principles and rules that determine how to ensure the protection of assets,
d) risk assessment is the overall process of identifying, analysing and evaluating risks,
e) privileged user is a user or person whose activity on a technical asset may have a significant impact on the security of a regulated service,

[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 Directive (EU) 2016/1148 (NIS 2 Directive).

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

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

h) information security management system the part of the obliged entity's management system based on an approach to assets risks, which provides for the establishment, implementation, operation, monitoring, review, maintenance and improvement of information and data security,

i) user is the natural or legal person or public authority using the asset,

j) top management is person or group of persons who control the obliged entity or the statutory body of the obliged entity; and

k) significant change is a change that has or may have an impact on cybersecurity and is determined based on established rules, procedures and criteria.

PART TWO

SECURITY MEASURES

§ 3

The obliged entity shall establish and implement security measures pursuant to this legal regulation within the scope of cybersecurity management established pursuant to § 13 of the Act (hereinafter referred to as the "established scope").

TITLE I

ORGANISATIONAL MEASURES

§ 4

Information Security Management System

(1) Within the information security management system, the obliged entity shall

a) set out 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, implement appropriate security measures to ensure the security of the regulated service,

c) manage risks in accordance with § 9,

d) establish and approve a security policy in relation to cybersecurity management, which includes the guiding principles, objectives of the information security management system, security needs, rights and obligations in relation to information security management, and, based on the security needs and the

results of the risk assessment, establish a security policy and security documentation in other areas as referred to in § 7,

e) ensure that a cybersecurity audit is carried out in accordance with § 17,
f) ensure an evaluation of the effectiveness of the information security management system at least annually, which shall include
    1. evaluation of the objectives of the information security management system aimed at ensuring the security of the regulated service,
    2. an assessment of the implementation of the risk management plan prepared pursuant to § 9(g),
    3. assessing the status of the information security management system, including reviewing risk assessments,
    4. assessing the results of cybersecurity audits and controls carried out in the area of cybersecurity,
    5. the results of previous evaluations of the effectiveness of the information security management system carried out pursuant to this point,
    6. an assessment of the impact of cybersecurity incidents on the services provided under § 16 and on the field of cybersecurity; and
    7. assessment of significant changes pursuant to § 12,
g) prepare a report on the review of the information security management system based on the evaluation of the effectiveness of the information security management system referred to in point (f),
h) continuously identify and subsequently manage significant changes in accordance with § 12,
i) update the information security management system and relevant documentation on the basis of
    1. findings of cybersecurity audits and controls,
    2. the results of the evaluation of the effectiveness of the information security management system,
    3. the impact of cybersecurity incidents on the services provided and
    4. in the context of major changes,
j) manage the operation and resources of the information security management system and record activities related to the information security management system and risk management; and
k) establish a process for managing exceptions to the rules established under point (d).

(2) In the event of failure to comply with the risk management obligation referred to in paragraph 1 (c), the obliged entity shall
    a) implement all the security measures required by this Decree,
    b) create with regards to the security measures referred to in point (a),
        1. a declaration of applicability pursuant to § 9(1)(f) and
        2. a risk management plan, as appropriate, in accordance with § 9(1)(g),
    c) take into account in the risk management plan
        1. significant changes,

2. changes to the specified scope under § X of the Act,
3. countermeasures under § X of the Act,
4. cybersecurity incidents, including those previously resolved,
5. the results of cybersecurity audits and controls; and
6. results of penetration testing and vulnerability scanning,

d) implement security measures in accordance with the risk management plan.

§ 5

Duties of top management

(1) Top management shall with regard to the information security management system

a) demonstrably participate in the training referred to in § 11(3)(a),
b) ensure the establishment of a security policy and objectives for the information security management system pursuant to § 4, compatible with the strategic direction of the obliged entity,
c) ensure the integration of the information security management system into the processes of the obliged entity,
d) ensure the availability of resources required for the information security management system,
e) inform employees of the importance of the information security management system and the importance of achieving compliance with its requirements with all concerned parties,
f) provide support to achieve the objectives of the information security management system,
g) guides and supports staff in developing the effectiveness of the information security management system,
h) participate in the preparation of the impact analysis referred to in § 16,
i) promotes continuous improvement of the information security management system,
j) supports those in security roles in promoting cybersecurity in their areas of responsibility,
k) ensure that rules are set for the appointment of administrators and persons who will fulfil security roles,
l) ensure that confidentiality is maintained for all relevant persons (e.g. administrators, persons in security roles, persons with access to sensitive information, contractors, etc.)
m) ensure that security role holders are provided with the appropriate authority and resources, including budgetary means, to fulfil their roles and related tasks; and
n) ensure testing of business continuity plans, recovery plans and processes related to the management of cybersecurity incidents.

(2) Top management is demonstrably familiar with

a) a 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 and
d) the results of cybersecurity audits and controls.

(3) Top management within the information security management system shall determine the composition of the cybersecurity management committee, security roles, their rights and responsibilities related to the information security management system.

(4) Meetings of the Cybersecurity Management Committee are held at regular intervals and a documented record of the proceedings is kept.

(5) The Cybersecurity Management Committee shall be composed of persons with appropriate authority and expertise for the overall management and development of the information security management system and persons significantly involved in the management and coordination of cybersecurity activities, and shall include at least one representative of senior management or their designee and the Cybersecurity Manager. The obliged entity for the cybersecurity management committee shall take into account the recommendations set out in Annex 6 to this Decree.

(6) Senior management will appoint a person to fill the security role
a) the Cybersecurity Manager,
b) the Cybersecurity Architect,
c) the Asset Guarantor and
d) the Cybersecurity Auditor.

(7) Senior management shall ensure the interchangeability of the security roles referred to in paragraph 6(a) and (b).

§ 6
Security roles

(1) The cybersecurity manager
a) is the security role responsible for the information security management system, which may be performed by a person who is trained for this role and demonstrates competence through experience in cybersecurity management or information security management
1. for at least three years, or
2. for one year if they have completed their studies at university,
b) is responsible for keeping senior management regularly informed of
1. the activities arising from the scope of its responsibilities and
2. the state of the information security management system,
c) may not be entrusted with roles responsible for the operation of the regulated service.

(2) The cybersecurity architect is a security role responsible for ensuring the design of the implementation of security measures to provide a secure architecture for a regulated service, and may be performed by a person who is trained for this role and demonstrates competence through experience in designing the implementation of security measures and ensuring the security architecture
a) for at least three years, or

b) for one year if they have completed their studies at university.

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

(4) The Cybersecurity Auditor

a) is the security role responsible for conducting the cybersecurity audit, which may be performed by a person who is trained for this role and demonstrates competence through experience conducting cybersecurity audits or information security management system audits
   1. for at least three years, or
   2. for one year if they have completed their studies at university,
b) ensures that the conduct of the cybersecurity audit is impartial and
c) shall not be assigned to other security roles.

(5) The obliged entity shall take into account the recommendations set out in Annex 6 to this Decree when designating persons in security roles.

§ 7

Management of security policy and security documentation

(1) Obliged entity in the management of security policy and security documentation

a) establish a security policy and maintain security documentation covering the areas listed in Annex 5 to this Decree; and
b) establish rules and procedures in the operational documentation that take into account relevant areas from the security policy and security documentation.

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

(3) The obliged entity shall regularly review the security policy and security documentation, ensuring that they are up-to-date and that their relevant areas are reflected in the operational documentation.

(4) The obliged entity shall designate a person responsible for regularly reviewing and updating the security policy, the security documentation and the consideration of their relevant areas in the operational documentation in accordance with paragraph 3.

(5) The security policy and security documentation must be managed in such a way that they are

a) available in electronic or paper form,
b) communicated within the obliged entity,
c) reasonably accessible to the parties concerned,
d) protected in terms of confidentiality, integrity and availability, and
e) maintained in such a way that the information contained therein is complete, legible, correct, easily identifiable and retrievable.

§ 8

Asset management

Obliged entity in accordance with the identification and recording of assets

a) establish a methodology for the identification and assessment of assets, including the determination of asset levels at least to the extent set out in Annex 1 to this Decree,

b) identify and record the guarantors of the assets,

c) assess the primary assets in terms of confidentiality, integrity and availability and classify them into the different tiers referred to in point (a),

d) assesses at least the areas listed in Annex 1 to this Decree as part of the assessment of primary assets,

e) identifies and records relevant links between assets,

f) assesses the supporting assets, taking into account in particular the links to the primary assets; and

g) establish and implement, for each asset level referred to in point (a), the protection rules necessary to ensure its confidentiality, integrity and availability, including in particular

   i) allowable uses of assets,

   ii) rules for handling assets,

   iii) rules for classifying information,

   iv) rules for asset labelling,

   v) exchange media management rules,

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

   vii) rules for determining the method of disposal of information and data and copies thereof and the disposal of technical assets that are carriers of information and data with regard to the level of assets in accordance with Annex 4 to this Decree.

§ 9

Risk management

(1) With regards to risk management in connection to § 8, the obliged entity shall

a) establish a methodology for identifying and assessing risks, including the establishment of criteria for risk acceptability,

b) identify relevant threats and vulnerabilities when identifying risks with respect to assets; in doing so, it shall consider in particular the categories of threats and vulnerabilities listed in Annex 3 to this Decree,

c) carry out risk assessments at regular intervals, at least once a year, and when significant changes occur,

d) take into account the relevant threats and vulnerabilities referred to in point (b) and assess the potential impact on assets, based on the asset assessment referred to in § 8; it shall assess those risks at least to the extent of Annex 2 to this Decree,

e) prepare a risk assessment report based on the risk assessment carried out pursuant to point (d),
f) prepare, on the basis of the security needs and the results of the risk assessment, a statement of applicability that includes a summary of all the security measures required by this Decree, which
    1. has not been applied, including a justification and a summary of the alternative security measures taken,
    2. has been applied, including the method of performance,
g) on the basis of the risk assessment carried out pursuant to point (d), prepare a risk management plan which shall include
    1. description of security measures,
    2. the objectives and benefits of security measures to manage individual risks,
    3. designating a person to ensure that security measures are in place to manage risks,
    4. the estimated human, financial and technical resources to implement the security measures,
    5. the required date for the implementation of the security measures,
    6. a description of the links between the risks and the relevant security measures; and
    7. how to implement security measures,
h) take account of the following in the risk assessment and risk management plan
    1. significant changes,
    2. changes to the specified scope under § X of the Act,
    3. countermeasures under § X of the Act,
    4. cybersecurity incidents, including those previously resolved,
    5. the results of cybersecurity audits and controls,
    6. results of penetration testing and vulnerability scanning and
    7. warning of the risk associated with the supplier under § X of the Act.

(2) The obliged entity shall implement security measures in accordance with the risk management plan.

(3) Risk management may be ensured by means other than those set out in point (d) of paragraph 1, provided that the obliged entity ensures the same or a higher level of risk management process.

§ 10

Management of suppliers

(1) The obliged entity shall
a) set rules for suppliers that take into account the requirements of the information security management system,
b) inform its suppliers of the rules referred to in point (a) and require compliance with those rules,
c) identify and records its major suppliers,

d) demonstrably inform its major suppliers in writing of their records under point (c).
e) manage the risks associated with suppliers,
f) ensure, in relation to the management of risks associated with major suppliers, that contracts concluded with major suppliers cover the relevant areas listed in Annex 7 to this Decree; and
g) regularly review the performance of contracts with major suppliers in terms of the information security management system.

(2) For major suppliers, the obliged entity shall furthermore
a) within the selection procedure and before the conclusion of the contract, carry out a risk assessment related to the performance of the subject of the selection procedure, as appropriate, in accordance with Annex 2 to this Decree,
b) determine, with regards to the contractual relations concluded, the methods and levels of implementation of security measures and determine the content of mutual contractual responsibility for the implementation and control of security measures,
c) carry out regular risk assessments and periodic reviews of the security measures in place for the services provided, using its own resources or those of a third party; and
d) ensure that risks and gaps are addressed in response to identified risks and gaps.

(3) The elements of demonstrable information referred to in paragraph 1(d) are
a) identification of the obliged entity,
b) identification of the regulated service,
c) identification of a major supplier,
d) notification of the fact that the supplier is a significant supplier to the obliged entity and
e) the content of the rules referred to in paragraph 1(a).

§ 11

Security of human resources

(1) The obliged entity shall establish a security awareness development plan with regards to human resources security management, taking into account the status and needs of the information security management system, with the aim of ensuring adequate education and improvement of security awareness, including the form, content and extent of the instruction and training referred to in paragraph 2.

(2) The obliged entity shall include in the security awareness development plan
a) briefing senior management on their responsibilities, security policy, particularly in the areas of information security management system and risk management,
b) educating users, administrators, security role holders and contractors about their responsibilities and the security policy,

c) the necessary theoretical and practical training of users, administrators and security role holders,
d) rules for creating secure passwords in accordance with § 20,
e) the relevant topics listed in Annex 8 to this Decree.

(3) Obliged entity shall in the framework of human resources security management
a) in accordance with the Security Awareness Development Plan, ensure that senior management is briefed on their responsibilities and security policy, particularly in the area of the information security management system and risk management, through initial and regular training,
b) in accordance with the security awareness plan, ensure that users, administrators, security role holders and contractors are educated about their responsibilities and the security policy through initial and regular training,
c) provide regular training for those in security roles in accordance with the security awareness plan, based on the current cybersecurity needs of the obliged entity,
d) in accordance with the Security Awareness Development Plan, ensure regular training and verification of security awareness of staff in accordance with their job description,
e) designate the persons responsible for the implementation of each of the activities listed in the Security Awareness Development Plan,
f) evaluate the effectiveness of the security awareness development plan, lessons learned, training and other security awareness activities,
g) ensure that users, administrators and persons in security roles are monitored for compliance with the security policy,
h) determine rules and procedures for dealing with breaches of established security rules by users, administrators and persons in security roles; and
i) in the event of termination of the contractual relationship with administrators and security role holders, ensure the handover of responsibilities.

(4) The obliged entity shall keep records of the instruction and training referred to in paragraph 3, which shall include the subject matter of the instruction and training, including a list of persons who have received the instruction and training.

§ 12

Change management

(1) With regards to change management for assets, the obliged entity shall
a) identify changes that have or may have an impact on cybersecurity,
b) set out the rules, procedures and criteria for determining significant changes and
c) for the changes identified under point (a), identify significant changes in accordance with point (b).

(2) With regards to significant changes the obliged entity shall
a) document their management,
b) conduct risk assessments,

c) take precautions to reduce any adverse impacts associated with significant changes,
d) update security and operational documentation,
e) ensure that they are tested before being put into operation; and
f) ensure the possibility of returning to the original state.

(3) On the basis of the results of the risk assessment referred to in paragraph 2(b), the obliged entity shall decide to carry out penetration testing; if he decides to carry out penetration testing, he shall proceed in accordance with § 25(6) of this Decree.

§ 13

Acquisition, development and maintenance

Obliged entity shall in connection with planned acquisition, development and maintenance of assets

a) manage risks in accordance with § 9,
b) control significant changes according to § 12,
c) establish security requirements in accordance with this Decree and its own security needs,
d) include the security requirements established under point (c) in the acquisition, development and maintenance project,
e) comply with and enforce the requirements laid down under point (c),
f) ensure separation of operational, backup, development, testing and other specific environments, and ensure protection of information and data contained therein,
g) where the purpose of the acquisition or development is to implement a technical asset using an authentication mechanism, in particular for the purpose of verifying the identity of users or administrators, comply with the requirements of § 20(3); and
h) where the acquisition or development is aimed at a technical asset using cryptographic algorithms, comply with the requirements under § 26(1)(a) and (3)(a).

§ 14

Access control

(1) Based on security and operational needs, the obliged entity shall control access to assets and take security measures to ensure the protection of access and authentication data used for identity verification pursuant to § 20 and § 21.

(2) The obliged entity shall furthermore, in the context of the management of access to assets
a) control 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) control the identifiers, access rights and permissions of technical asset accounts,
d) establish security measures to control access of technical assets to other assets,

e) implement the security measures necessary for the safe use of mobile devices and other similar technical assets, including, where appropriate, security measures related to the use of technical assets that are not under the control of the obliged entity,
f) limit the assignment of administrative and privileged privileges to the level necessary to perform the job,
g) restrict and control the use of software and equipment that may be capable of overriding system or application controls,
h) enforce that established rules and procedures are followed when using private authentication information and mechanisms,
i) assign and removes access permissions in accordance with the access control policy,
j) periodically review all access permissions, including grouping and role assignments,
k) ensure that access privileges are removed or changed without delay when changing positions or assignments based on groups and roles,
l) ensure that access privileges are removed or changed without delay upon termination or change of the contractual relationship,
m) document the granting and revoking of access permissions, and
n) use the identity management and authentication tool according to § 20 and the access authorisation management tool according to § 21.

§ 15

Cybersecurity event and incident management

(1) With regard to cybersecurity event and incident management, the obliged entity shall
a) establish processes, rules and procedures for detecting, recording and evaluating cybersecurity events in accordance with §s 22 to 24 and managing cybersecurity incidents,
b) assign responsibilities for
   1. detecting, recording and evaluating cybersecurity events and
   2. coordination and management of cybersecurity incidents,
c) defines and follows rules and procedures for identifying, collecting, obtaining and preserving credible evidence needed for cybersecurity incident analysis,
d) ensure the detection of cybersecurity events in accordance with § 22,
e) ensure that users, administrators, security role holders, other employees and contractors report unusual behaviour of technical assets and suspected vulnerabilities,
f) ensure the assessment of cybersecurity incidents, which must decide whether they should be classified as cybersecurity incidents,
g) ensure that cybersecurity incidents are managed according to established procedures,

h) take security measures to avert and mitigate the impact of a cybersecurity incident,
i) report cybersecurity incidents pursuant to § 16 of the Act,
j) keep records of cybersecurity incidents and their management,
k) investigate and determine the causes of a cybersecurity incident and
l) evaluate the effectiveness of the response to the cybersecurity incident and, based on the evaluation, determine the necessary security measures or update existing security measures to prevent a recurrence of the cybersecurity incident.

(2) In addition, the obliged entity shall use the tools referred to in §s 22 and 24 to detect and evaluate cybersecurity events.

§ 16

Business continuity management

(1) With regards to business continuity management, the obliged entity shall

a) sets out the methodology for carrying out the impact analysis,
b) evaluate and document the potential impact of cybersecurity incidents through an impact analysis and take into account the risk assessment under § 9, which assesses the potential risks associated with threats to business continuity,
c) on the basis of the outputs of the impact analysis and risk assessment referred to in point (b), set business continuity management objectives by identifying
    1. the minimum level of service that is acceptable for the use, operation and management of the regulated service,
    2. the recovery time during which the minimum level of service provided by the regulated service will be restored following a cybersecurity incident; and
    3. data recovery point as the time period in which data must be recovered after a cybersecurity incident or failure,
d) establish a business continuity management policy that includes the fulfilment of the objectives referred to in point (c) and sets out the rights and obligations of administrators and persons in security roles,
e) develop, update and regularly test business continuity plans and recovery plans related to the provision of the regulated service,
f) implement security measures to increase resilience in accordance with § 27; and
g) review the impact analysis at least once a year and update it if necessary.

(2) The objectives of continuity management under paragraph 1(c) of this provision are the time and quality of regulated service established under § 34 of the Act. The specified time is the recovery time under paragraph 1(c)(2) of this provision and the specified quality of regulated service is the minimum level of service provided under paragraph 1(c)(i) of this provision.

§ 17

Cybersecurity audit

(1) The obliged entity shall establish a plan for conducting a cybersecurity audit.

(2) Obliged entity shall in the context of a cybersecurity audit

a) assess whether the security measures required by the Cybersecurity Act and this Decree have been implemented,

b) assess the compliance of the security measures in place with legislation, internal rules, other regulations, contractual obligations and best practice relating to the regulated service; and

c) audit and document compliance with the rules and procedures set out in the security policy, including a review of technical compliance and previously identified corrective actions in accordance with paragraph 4.

(3) The obliged entity shall take into account the results of the cybersecurity audit referred to in paragraph 2 in

a) risk management plan,

b) declaration of applicability and

c) security awareness development plan.

(4) The obliged entity shall determine the corrective measures, if any, to comply with the requirements referred to in paragraph 2.

(5) The cybersecurity audit referred to in paragraph 2 shall be carried out

a) in the case of significant changes, within their scope,

b) at regular intervals of at least 2 years and

c) in accordance with the cybersecurity audit plan.

(6) Where, in justified cases, it is not possible to carry out the audit at the interval referred to in paragraph 5(b) in its entirety in accordance with paragraph 2, the cybersecurity audit may be carried out continuously in systematic units. In such a case, the audit shall be carried out in its entirety in accordance with paragraph 2 within 5 years at the latest.

(7) The cybersecurity audit must be conducted by a person meeting the conditions set out in § 6(4) who independently assesses the correctness and effectiveness of the security measures in place.

TITLE II

TECHNICAL MEASURES

§ 18

Physical security

With regards to physical security, the obliged entity shall

a) prevent damage, theft, misuse of assets and interruption of regulated service,

b) establish a physical security perimeter bounding the area in which information and data are stored or processed or in which the technical assets of the regulated service are located,

c) document the individual physical security perimeters referred to in point (b) with regard to the assessment of the deployed technical assets and divide them into individual physical protection levels,

d) for each physical security perimeter established pursuant to point (c), take appropriate physical security measures with respect to its level of physical protection to

1. prevent unauthorised entry,
2. prevent damage and tampering,
3. ensure physical protection at the level of objects and within objects,
4. ensure detection of breaches of the physical security perimeter and
5. record entries and accesses to the physical security perimeter.

§ 19

Security of communication networks

To protect the security of the communication network, including its network perimeter, the obliged entity shall

a) ensure the segmentation of the communication network, including the separation of operational, backup, development, testing and other specific environments,

b) ensure communication management within the communication network,

c) provide remote access control to the communication network,

d) ensure remote management of technical assets,

e) in the context of communications management, remote access and remote administration, permit only such communications as are necessary for the proper provision of the regulated service,

f) use cryptographic algorithms regulated in § 26, ensure confidentiality and integrity in the transmission of information and data within the communication network; and

g) use a tool that ensures the integrity of the communication network is protected.

§ 20

Identity management and authentication

(1) The obliged entity shall use the tool to manage and authenticate the identity of administrators, users and technical assets of the regulated service.

(2) The tool for managing and verifying the identity of administrators, users and technical assets ensures

a) identity verification before starting their activities,
b) managing the number of possible failed login attempts,
c) resilience of stored and transmitted authentication data to threats and vulnerabilities that could compromise its confidentiality or integrity,
d) re-authentication of identity after a specified period of inactivity,

e) maintaining confidentiality when creating default authentication credentials and when restoring access; and
f) centralised identity management with respect to links between assets.

(3) The obliged party shall use an authentication mechanism based on multi-factor authentication with at least two different types of factors to verify the identity of administrators, users and technical assets.

(4) The obliged entity shall keep a record of technical assets, accounts and authentication mechanisms that do not meet those requirements, including a justification, until the requirements for the authentication of administrators, users or technical assets under paragraph 3 have been met.

(5) The obliged entity shall use cryptographic key or certificate authentication until the requirement for identity verification of administrators, users or technical assets using an authentication mechanism based on multi-factor authentication with at least two different types of factors as referred to in paragraph 3 is met.

(6) The obliged entity shall use a cryptographic key or certificate-based authentication mechanism to authenticate the identity of administrators, users and technical assets using an account identifier and password-based authentication tool until the requirement for identity authentication of administrators, users and technical assets is met in accordance with paragraph 5, and the tool shall enforce the following rules

a) password lengths of 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 passwords, with no less than 30 minutes between password changes,
e) mandatory password changes at intervals of no more than 18 months,
f) not allowing users and administrators
   1. choose simple and frequently used passwords,
   2. create passwords based on multiple repeating characters, login name, email, system name or similar; and
   3. reuse previously used passwords with a memory of at least 12 previous passwords.

(7) The obliged entity shall, in accordance with paragraph 6

a) create a random default password or identifier used to create or restore access; and
b) ensure that the default password of the technical asset is changed without delay,
c) ensure that users and administrators change their default passwords immediately after their first login,
d) ensure that, as part of the identity authentication of the technical asset, its new password is created with a random string of upper and lower case letters, numbers and special characters; and

e) immediately force a change of the access password in case of a reasonable suspicion of its compromise.

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

(9) The obliged entity must enforce the following rules for an administrator account designed specifically for recovery from a cybersecurity incident

a) promptly forces a change in the default password,
b) The password must be a random string of upper and lower case letters, numbers and special characters,
c) Password length must be at least 22 characters,
d) the password must be stored securely,
e) The account and its password may only be manipulated by authorised persons and only in cases of absolute necessity,
f) the password must be enforced to be changed after use, upon any change of responsible persons, or at intervals of no more than 18 months; and
g) records the manipulation and attempted manipulation of this account and its password.

§ 21
Access permission management

With regard to access permission management, the obliged entity shall

a) use a centralised tool with respect to the links between assets,
b) control the permissions for access to individual assets and
c) control permissions for reading data, writing data, and changing permissions.

§ 22
Detection of cybersecurity events

(1) The obliged entity shall use a cybersecurity event detection tool that provides, within the communication network, that ensures

a) verification and control of transmitted data within 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 shall use a centrally managed tool with respect to the links between assets for the detection of cybersecurity events, which ensures for each relevant technical asset

a) continuous and automatic protection against malicious code,
b) managing and monitoring the use of removable devices and data carriers,

c) control of automatic content launching, 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) detecting cybersecurity events over technical assets and
g) detection based on the behaviour of technical assets, administrators and users.

(3) The obliged entity shall regularly and without delay update the tool used pursuant to paragraphs 1 and 2, including its settings and detection rules.

§ 23

Recording of events

(1) The obliged entity shall identify the technical assets for which the recording of security and relevant operational events is performed on the basis of an assessment of assets and security needs.
(2) The obliged entity shall, in accordance with paragraph 1, record security 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 entity shall update the range of technical assets determined in accordance with paragraph 1 at regular intervals and when significant changes occur.
(4) The obliged entity shall ensure the continuous synchronisation of the uniform time of technical assets.
(5) The obliged entity shall, in particular, record the following information about the event in the context of the recording of events referred to in paragraph 2
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 originator's equipment and
f) the success or failure of the activity.
(6) The obliged entity shall ensure that the network identification referred to in paragraph 5(c) to (e) is unambiguous in the event of a change in the communication network.
(7) In order to ensure the confidentiality and integrity of the information obtained pursuant to paragraph 2, the obliged entity shall ensure that it is protected against unauthorised reading and any alteration.
(8) The obliged entity shall, as part of the recording of events referred to in paragraph 2, record in particular
a) logging in and out of all accounts, including failed attempts,

b) the performance and unsuccessful attempt to perform the privileged activity,

c) manipulation and failed attempt to manipulate accounts, permissions and rights,
d) failure to carry out activities due to lack of access rights or authorisation,
e) commencement and termination of technical asset activities,
f) critical and error messages of technical assets,
g) access and failed attempts to access event logs,
h) tampering and unsuccessful attempt to tamper with event records,
i) change and unsuccessful attempt to change the settings of the event logging tools and
j) other user activities that may affect the security of the regulated service.

(9) The obliged entity shall use a central tool with respect to links between assets to collect and store records of events recorded in accordance with paragraph 2.

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

§ 24

Evaluation of cybersecurity events

(1) The obliged entity shall use the tool for continuous assessment of cybersecurity events detected pursuant to § 22 for
a) collecting, searching and grouping related records to detect cybersecurity events,
b) continuous provision of information on detected cybersecurity events, early warning to designated security roles, and
c) evaluating cybersecurity events to identify cybersecurity incidents.

(2) The obliged entity shall, as part of the use of the instrument in accordance with paragraph 1, ensure
a) reducing instances of incorrect or unwanted assessment of cybersecurity events,
b) regular updates of the tool settings, including its rules for detecting and evaluating cybersecurity events; and
c) regular updates of rules for the continuous provision of information on detected cybersecurity events, including early warning to designated security roles.

(3) The obliged entity shall use the information obtained by the cybersecurity event assessment tool to optimally set up the regulated service's information security management system and implement security measures.

§ 25

Application security

(1) To ensure the security of the regulated service, the obliged entity shall use technical assets that are supported by the manufacturer, supplier or other person and shall ensure that security updates issued for these assets are applied without delay.

(2) Until the time of compliance with paragraph 1, the obliged entity shall register the technical assets that are no longer supported by the manufacturer, supplier or other person and shall implement security measures that guarantee a similar or higher level of security for those technical assets.

(3) The obliged entity shall also ensure, as part of application security, the permanent protection of applications, information, transactions and transmitted session identifiers against

a) unauthorised activity and
b) by denying the actions taken.

(4) The obliged entity shall perform regular vulnerability scans 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 entity shall take the results of the vulnerability scans into account in the risk management framework pursuant to § 9 and shall implement security measures based on the results.

(6) The obliged entity carries out 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 they are put into operation and
c) in connection with a significant change pursuant to § 12(3).

(7) The obliged entity shall take into account the results of penetration testing in the framework of risk management pursuant to § 9 and shall implement security measures based on the results found.

(8) The obliged entity shall retest a finding identified by a vulnerability scan or penetration testing to verify the functionality of the security measures in place.

(9) The obliged entity shall, in accordance with paragraph 6(a), carry out penetration testing on a regular basis and at least once every two years.

(10) The obliged entity may, in justified cases where he cannot carry out penetration testing within the scope or interval set out in paragraph 9, divide such penetration testing into systematic units. In such a case, the penetration testing shall be carried out within the scope set out in paragraph 6 within 5 years at the latest.

§ 26

Cryptographic algorithms

(1) For ensuring the protection of technical assets and their communication, the obliged entity shall

a) use currently robust cryptographic algorithms,
b) promote the secure handling of cryptographic algorithms and
c) take into account the recommendations and methodologies in the field of cryptographic algorithms issued by the Office and published on its website.

(2) The obliged entity shall, in accordance with paragraph 1, ensure the safe

a) voice, audio-visual and text communication, including email communication and
b) emergency communication within the organisation.

(3) In the case of the use of cryptographic keys and certificates for the protection of technical assets and the communication network, the obliged entity shall use
   a) only the currently resistant cryptographic keys and certificates, and
   b) a key and certificate management system that
      1. ensure the generation, distribution, storage, modification, restriction 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 entity shall put in place security measures to ensure the availability of the regulated service to ensure
   a) the availability of the regulated service according to the objectives set out under § 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) In order to ensure the availability of the regulated service in accordance with paragraph 1, the obliged entity shall create regular backups of the settings of technical assets, information and data necessary in particular for the purposes of restoring the regulated service in the event of a cybersecurity incident.

(3) The obliged entity shall, for the backups created pursuant to paragraph 2, ensure that
   a) regular testing of their integrity, availability and recoverability,
   b) documenting the results of the tests carried out pursuant to paragraph 3(a),
   c) protection of stored backups and the data contained therein against breaches of their integrity and confidentiality, in particular by encrypting such backups in accordance with § 26; and
   d) protect stored backups and the data contained in them from accessibility breaches.

(4) In order to limit the spread of a cybersecurity incident and reduce its impact, the obliged entity shall separate the backup environment from other environments as referred to in § 19(a).

§ 28

Security of industrial, control and similar specific technical assets

In addition, to ensure the cybersecurity of industrial, control and similar specific technical assets, the obliged entity shall use tools and implement security measures to ensure

a) restrictions on physical access to industrial, control and similar specific technical assets,

b) limitations on the authorisation of access to industrial, control 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) limiting remote access and remote management of industrial, control and similar specific technical assets,

e) protection of individual industrial, control and similar specific technical assets against exploitation of threats and known vulnerabilities; and

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

PART THREE

FINAL PROVISIONS

§ 29

Transitional provisions

Regulated service providers who, on the day preceding the entry into force of this Decree, were an authority or person pursuant to § 3 of Act No. 181/2014 Coll., on Cybersecurity, obligated to requirements in the area of the introduction and implementation of security measures pursuant to Decree No. 82/2018 Coll, Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (the Cybersecurity Decree), as amended before the date of entry into force of this Decree, and who, on the date of entry into force of this Decree, fulfil the criteria for identification of at least one regulated service, shall introduce and implement, to the extent provided for by the Cybersecurity Act, security measures pursuant to Decree No. 82/2018 Coll, Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (the Cybersecurity Decree), as in force before the date of entry into force of this Decree.

PART FOUR
EFFECTIVENESS
§ 30
Effectiveness

This Decree shall enter into force on dd.mm.yyyy.

Director:

Ing. Lukáš Kintr v. r.

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

Identification and evaluation of assets

1) When identifying the primary assets of a regulated service, it is useful to first identify its purpose. From the purpose it is possible to derive the service type asset. It is then appropriate to identify what information the service works with and derive the primary assets in form of information.
2) The identification of supporting assets must be based on the system architecture of the regulated service and in particular take into account the links to primary assets. The obliged entity should choose the detail of the supporting assets such that it is able to adequately identify and manage the risks associated with the assets.
3) Asset guarantors are identified based on their job title and their process and asset expertise. For asset management purposes, the asset guarantor must be able to assess the asset on the basis of potential impacts.
4) In this case, the four-level rating scales shown in Tables 1, 2 and 3 are used to evaluate the assets, also the impact of an information security breach on each asset is evaluated. It is recommended that the obliged party tailor these asset rating levels in the scale to its needs. An obliged entity may use a different number of asset rating scales than those specified in this Annex, provided that they maintain clear links between the asset rating method they use and the asset rating scales and levels specified in this Annex.
5) With regards to primary assets, at least the areas listed in *Table 4 - Primary asset evaluation areas* must be taken into account.
6) When evaluating supporting assets, it is necessary to take into account the links between supporting and primary assets. For example, one of the following can be used
   a) supporting assets assume the values of primary assets,
   b) supporting assets are evaluated individually with respect to the value of the primary assets,
   c) supporting assets assume the values of primary assets through a suitably chosen formula.
7) The rules on asset protection also apply to paper documents, removable devices and data carriers that are electronic copies of the originals.

Table 1: Confidentiality rating scale

Level	Description	Examples of asset protection requirements
Low	The asset is publicly available or have been designated for publication. A breach of the confidentiality of the asset does not jeopardize the legitimate interests of the obliged entity.	No protection is required. In the case of sharing such an asset with third parties and using the Traffic Light Protocol (TLP) classification, the TLP:CLEAR designation is used.

		Disposal/deletion of the asset at the Low level - see Annex 4.
Medium	The asset is not publicly available and constitute the know-how of the obliged entity, the protection of the asset is not required by any legal regulation or contractual arrangement.	Access management means are used to protect confidentiality. In the case of sharing such an asset with third parties and using the TLP classification, the TLP:GREEN or TLP:AMBER designation is mainly used. Asset disposal/deletion at Medium level - see Annex 4.
High	The asset is not publicly accessible and its protection is required by law, other regulations or contractual arrangements (e.g. trade secrets, personal data).	To protect confidentiality, means are used to ensure that access is controlled and recorded. Information transmissions over communication networks are protected by cryptographic means. In the case of the sharing of such an asset with third parties and the use of TLP classification, the TLP:AMBER or TLP:AMBER+STRICT designation is used in particular. Disposal/deletion of asset at High level - see Annex 4.
Critical	The asset is not publicly accessible and require a higher level of protection than the previous category (e.g. strategic trade secrets, special categories of personal data).	To protect confidentiality, means are used to ensure that access is managed and recorded. In addition, protection methods to prevent misuse of assets by administrators are used. Information transmissions are protected by cryptographic means. In the case of sharing such an asset with third parties and using the TLP classification, the TLP:RED designation is used in particular. Asset disposal/deletion at the Critical level - see Annex 4.

Table 2: Integrity rating scale

Level	**Description**	**Examples of asset protection requirements**
Low	The asset does not require integrity protection. A breach of the integrity of the asset does not compromise the legitimate interests of the obliged entity.	No protection is required.

Medium	The asset may require integrity protection. A breach of the integrity of an asset may lead to damage to the legitimate interests of the obliged entity and may result in less severe impacts on the primary assets.	Standard tools are used to protect the integrity.
High	The asset requires integrity protection. A breach of the integrity of the asset leads to damage to the legitimate interests of the obliged entity with significant effects on the primary assets.	To protect the integrity, special means are used to track the history of changes made and to record the identity of the person making the change. The integrity of information transmitted over communication networks is protected by cryptographic means.
Critical	The asset requires integrity protection. A breach of integrity leads to very serious damage to the legitimate interests of the obliged entity with direct and very serious effects on the primary assets.	Special means of uniquely identifying the person making the change are used to protect the integrity.

Table 3: Accessibility rating scale

Level	**Description**	**Examples of asset protection requirements**
Low	Disruption to the availability of the asset is not important and in the event of an outage, a longer recovery period (up to approximately 1 week) is normally tolerated.	Regular backups are sufficient to protect availability.
Medium	The disruption of the availability of the asset should not exceed the duration of the working day, a longer outage leads to a possible threat to the legitimate interests of the obliged entity.	Common backup and recovery methods are used to protect availability.
High	Disruption to the availability of an asset should not exceed a few hours. Any outage must be dealt with immediately as it leads to a direct threat to the legitimate interests of the obliged entity. Assets are considered to be very important.	Backup systems are used to protect availability, and service restoration may be subject to operator intervention or replacement of technical assets.
Critical	Disruption of the availability of an asset is not permitted and even short-term unavailability	Backup systems are used to protect availability and service restoration is short-term and automated.

	(within a few minutes) leads to a serious threat to the legitimate interests of the obliged entity. Assets are considered critical.	

Table 4 Primary asset evaluation areas

When assessing primary assets, at least relevant areas of the following need to be assessed

Area	Example
(a) the extent and relevance of the personal data, special categories of personal data	Leakage of personal data of an individual.
(b) the extent of any legal duties or other obligations or business secrets involved	Infringement of the obligation to publish documents on an electronic official notice board which must be accessible by remote access at all times. Breach of contract and resulting penalties. Trade secret leak. Violations of legislation and resulting fines.
(c) the extent of disruption to 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 loss	Unavailability of invoice information based on the unavailability of the economic system. Unavailability of information about potential business opportunities and the resulting lost profits. The unavailability of websites, for example, can lead to the public not being informed about important facts (floods, environmental disasters, etc.).
(e) impacts on the provision of essential services	Disruption of all information and services related to the regulated service and the organization's core business objective (purpose for existence).
(f) the extent of disruption to normal activities	Disruption of personnel, economic, building and fleet management activities, inability to receive data messages, etc.
(g) the impact on the preservation or protection of reputation	Non-compliance. Leaked internal information.
(h) impacts on the security and health of persons	Inability to provide basic income, food, access to health care, freedom, etc. Potential for injury and loss of life.

(i) impacts on international relations	Leaks from foreign partners. A leak from a partner that is part of an international concern.
(j) impacts on users of the information and communication system	Loss of user access to the service due to its unavailability.

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

Risk assessment

1) The unambiguous determination of the risk identification function is an essential part of the methodology for risk assessment according to § 9 of this Decree.
2) The risk value is most often expressed as a function of the asset value, threat and vulnerability.
3) For example, the following function can be used to assess risk:
   Risk = asset value × threat × vulnerability.
4) In this case, the value of the asset is derived from the asset evaluation in Annex 1 to this Decree.
5) In case the obliged entity uses a risk assessment method that does not distinguish between threat and vulnerability assessment, the scales for threat and vulnerability assessment can be merged, i.e. scenarios combining threat and vulnerability can be created. The merging of scales should not lead to a loss of the ability to distinguish between threat and vulnerability levels. For this purpose, for example, a commentary can be used that clearly expresses both the threat level and the vulnerability level. A similar approach shall be followed where the obliged entity uses a different number of levels to evaluate assets, threats, vulnerabilities and risks.

Table 1: Threat rating scale

Level	Description
Low	The threat is non-existent or unlikely. The threat is not expected to be realised more than once every 5 years.
Medium	The threat is unlikely to probable. The threat is expected to be realised in the range of 1 to 5 years.
High	The threat is likely to very likely. The threat is expected to be realised in the range of 1 month to 1 year.
Critical	The threat is very likely to more or less certain. The threat is expected to occur more than once a month.

Table 2: Vulnerability rating scale

Level	Description
Low	The vulnerability does not exist or exploitation of the vulnerability is unlikely. Security measures are in place to detect potential vulnerabilities or possible attempts to exploit them early.
Medium	Exploitation of the vulnerability is unlikely to likely. Security measures are in place and their effectiveness is regularly monitored. The ability of security measures to detect potential vulnerabilities or possible attempts to overcome security measures in a timely manner is limited. There are no known successful attempts to overcome the security measures.
High	Exploitation of the vulnerability is likely to be very likely. Security measures are in place, but their effectiveness does not cover all necessary aspects and is not regularly monitored. Partial successful attempts to overcome security measures are known.
Critical	Exploitation of the vulnerability is very likely to more or less certain. Security measures are not implemented or their effectiveness is severely limited. There is no check on the effectiveness of security measures. There are known successful attempts to overcome security measures.

Table 3: Risk rating scale

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 initiated to eliminate it.
Critical	The risk is unacceptable and steps must be taken immediately to eliminate it.

6) If the value of the risk is higher than the threshold of acceptability, appropriate security measures must be implemented to reduce the value of the risk or eliminate the risk and ensure the required level of information security. The methods for risk management are as follows

   a) acceptance of risk,

   b) risk reduction and elimination,

   c) risk avoidance, or

   d) risk transfer or risk sharing.

Annex No. 3 to Decree No. XXXX Coll.
Vulnerabilities and threats

Please note: This appendix contains only selected categories of vulnerabilities and threats. The obliged entity shall identify specific threats and vulnerabilities according to its needs and specificities. The identification of specific vulnerabilities and threats is the responsibility of the obliged entity.

Vulnerabilities

1. Inadequate maintenance of assets,
2. Obsolescence of assets,
3. Insufficient perimeter protection,
4. Insufficient security awareness among users, administrators, security role holders, suppliers and senior management,
5. Insufficient backup,
6. Inappropriate access permission settings,
7. Insufficient procedures and processes for detecting cybersecurity events and identifying cybersecurity 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 establishment of security rules and procedures, inaccurate or ambiguous definition of rights and obligations of users, administrators, security role holders, contractors and top management,
10. Insufficient asset protection,
11. Inappropriate security architecture
12. Insufficient independent scrutiny,
13. Incapacity to detect misconduct in a timely manner by users, administrators, security role holders, contractors and senior management,
14. Shortage of staff with the necessary level of expertise,
15. Location of the asset outside physical control (e.g. in a foreign country),
16. Location of the asset in the territory of a State of which the obliged entity has insufficient knowledge of the legal environment,
17. Vulnerabilities discovered during vulnerability scanning and penetration testing.

Threats

1. Violation of security policy, unauthorized activities, misuse of privileges by users, administrators, security role holders, contractors and senior management
2. Damage or failure of technical and/or software equipment
3. Identity abuse
4. Use of the software in violation of the license terms
5. Malicious code
6. Physical security breaches
7. Interruption of electronic communications services or electricity supply
8. Misuse or unauthorised modification of information

9. Loss, theft or damage to the asset
10. Failure by the supplier to comply with a contractual obligation
11. Misconduct by users, administrators, security roles, suppliers and senior management,
12. Misuse of internal resources, sabotage
13. Prolonged interruption in the provision of electronic communications services, electricity supply or other essential services
14. Staff with insufficient professional knowledge
15. Targeted cyber-attack using social engineering, use of espionage techniques
16. Misuse of removable technical data carriers
17. Electronic communication hacking (interception, modification)
18. Dependence on suppliers
19. Abuse of state power to access assets
20. Disclosure or transfer of assets at the request of the State

Annex No. 4 to Decree No. XXXX Coll.
Data disposal

1) This Annex specifies the obligations of the obliged entity to define the means of disposal of information and data and copies thereof and the disposal of technical assets that are carriers of information and data with respect to the level of the assets.
2) The obliged entity shall lay down rules on how to dispose of information and data and copies thereof and how to dispose of technical assets that are carriers of information and data in accordance with this Annex. This is without prejudice to obligations under other legislation. 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 regard to the level of assets, shall be chosen.
3) The rules for the disposal of information and data should be set proportionate 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 or not the information and data carriers are under the control of the organisation,
   d) whether the information and data are part of a dedicated or shared environment,
   e) who will perform the destruction of information and data (e.g., an internal employee or contractor),
   f) availability of equipment and tools for disposal,
   g) the capacity of disposed information and data carriers,
   h) whether trained staff are available,
   i) time-consuming disposal,
   j) the cost of disposal with respect to tools, training, validation and reuse of the information and data carrier

k) possible ways of destroying information and data (for example, by destroying the medium, overwriting the medium several times, making it unreadable, encrypting it, etc.),

l) the applicable methods of disposal of information and data in relation to the state of the information carrier (for example, if the device is damaged, it will not be possible to use the data overwriting option, 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 copies thereof

a) Removal

1) A method of disposing of information and data media so that it is inaccessible (e.g., removing a data file, discarding a printed document in the trash).

2) It is the least secure way to dispose of information and data. If the information and data carrier is recovered, the information and data can be recovered with some effort.

3) This method is not applicable to non-rewritable digital information and data carriers.

4) Applicable method for the level of confidentiality of the asset (based on Annex 1): low.

b) Overwriting

1) The method of disposal consists of 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 may be replaced or combined with secure disposal of the cryptographic keys to the encrypted information.

4) This method is not suitable for damaged media, media that cannot be overwritten, or media with large capacities.

5) Applicable method for the level of confidentiality of the asset (based on Annex 1): low to critical.

c) Physical destruction of the information and data carrier

1) A method of disposal consisting in the destruction of the information and data carrier, or in the dismantling of the equipment and subsequent destruction of the information and data carrier (by mechanical, chemical or thermal action).

2) It is the most secure method of information and data disposal. After physical destruction, the information and data carrier cannot be reused for its original purpose. The original information and data cannot be recovered even with a large amount of resources and effort.

3) Applicable disposal method for the asset confidentiality level (based on Annex 1): medium to critical.

Example of possible disposal methods according to the level of confidentiality of the asset (based on Annex 1)

<table>
<tr><td></td><td colspan="4">Permissible method of disposal by asset level</td></tr>
<tr><td>Information carrier</td><td>1. Low</td><td>2. Medium</td><td>3. High</td><td>4. Critical</td></tr>
<tr><td>Information and data in human-readable media (printed documents, notes, etc.).</td><td>Disposal: Disposal in the garbage.</td><td>Overwriting: Blackening.

Physical destruction: the destruction of the information and data carrier using a shredding machine.</td><td colspan="2">Physical disposal:
Destruction of the information and data carrier by using a shredding machine with longitudinal and transverse cuts, burning or disintegration.</td></tr>
<tr><td>Mobile devices (mobile phones, tablets, laptops, etc.).</td><td>Removal: erase information and data, reset the device to factory settings.</td><td>Overwriting: For devices with encrypted storage - remove 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, etc.).</td><td rowspan="2">Removal: Erase information and data, reset to factory settings.</td><td rowspan="2">Overwriting: Removing and overwhelming artificial events (artificial network traffic, test print jobs, etc.).</td></tr>
<tr><td>Office equipment (scanners, printers, fax)</td></tr>
<tr><td>Internal and external storage (magnetic tapes, HDDs, SSDs, CDs, DVDs, removable media, etc.).</td><td rowspan="2">Delete: delete information and data at the file system level.</td><td>Overwriting: Overwriting information and data. In the case of encrypted media, the alternative is secure disposal of cryptographic keys</td><td colspan="2" rowspan="2">Physical destruction: destruction of the information and data carrier.</td></tr>
<tr><td>Physical disposal.</td></tr>
<tr><td>Outsourcing and the cloud</td><td colspan="4">The permissible method of disposal of information and data should be set out in a contractual arrangement.</td></tr>
<tr><td></td><td>Removal:</td><td>Overwriting:</td><td>Overwriting:</td><td></td></tr>
</table>

	Delete all files including previous versions.	The use of storage medium level encryption and secure disposal of cryptographic keys. Alternatively, in the case of a dedicated storage medium, the information and data can be overwritten after the end of the service.	Using 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 FIPS 140-2 Level 2). Upon termination of service, the top access key is destroyed and the information and data is overwritten.	Overwriting/physical disposal: method used see level "3. High" or used dedicated storage capacity. At the end of service, performed a total sanitization of all used storage media per the above lines for level critical.

Annex No. 5 to Decree No. XXXX Coll.
Content of the security policy and security documentation

1. Security Policy
   1.1. Information Security Management System Policy
      a) Objectives, principles and needs of an 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 activities of the 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 action and improvement of the information security management system.
   1.2. Organisational Security Policy
      a) Determine the composition of the Cybersecurity Management Committee and its rights and responsibilities.
      b) Identification of security roles and their rights and responsibilities.
      c) Determination of the rights and obligations of users and administrators.
      d) Requirements for the separation of activities of individual security roles.
      e) Requirements for separation of security and operational roles.
   1.3. Security Policy Management and Documentation Policy

a) Designation of a person responsible for periodically reviewing and updating 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) Rules for the protection of individual asset levels

1) allowable uses of assets,

2) rules for handling assets,

3) rules for classifying information,

4) rules for asset labelling,

5) exchange media management rules,

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

7) rules for determining how to dispose of data, operational data, information and copies thereof, or the disposal of technical data media, taking into account the level of assets.

d) 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 supplier selection.

b) Rules for assessing risks related to suppliers.

c) Rules and principles for determining major suppliers.

d) Contract details taking into account relevant requirements for the supplier arising from security policies and security documentation.

e) The elements of the service level agreement and the manner and level of implementation of security measures and the determination of mutual contractual responsibilities.

f) Rules for carrying out checks on the implementation of security measures.

g) Rules for evaluating suppliers.

h) Rules for keeping records of contact details of suppliers responsible for system and technical support.

i) Rules for eliminating dependence on a single supplier (especially vendor lock-in and exit strategy issues).

1.7. Human Resources Security Policy

a) Rules and procedures for the development of security awareness and methods of its evaluation

1) ways and forms of user education and training,

2) ways and forms of instruction and training of administrators,
3) ways and forms of instruction and training of persons in security roles,
4) methods and forms of instruction and training of senior management
5) ways and forms of instructing suppliers

b) Security training for new employees.

c) Establishing timeframes for periodic refresher training for users, administrators, security role holders and senior management.

d) Rules and procedures for dealing with breaches of the information security management system security policy.

e) Rules and procedures for termination of employment or change of position
1) the return of assets entrusted to them and the withdrawal of rights on termination of the employment relationship,
2) changing access permissions when changing job roles.
3) handover of responsibilities when changing jobs or terminating employment relationships with administrators or security role holders

f) Rules of basic cyber hygiene.

g) Rules for creating and using passwords.

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

i) Method of keeping track of training.

1.8. Policy for the safe behaviour of users, administrators and persons in security roles

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

b) Rules and procedures for the secure handling of passwords and other authentication mechanisms.

c) Rules and procedures for the safe use of electronic mail and Internet access.

d) Rules and procedures for secure remote access.

e) Rules and procedures for safe behaviour on the internet and social networks.

f) Rules and procedures for reporting unusual behaviour of technical assets and suspected vulnerabilities.

1.9. Safe Use of Mobile Devices Policy

a) Rules and procedures for the safe handling and use of mobile devices on and off the internal communications network.

b) Rules and procedures for ensuring the security of devices not under the control of the obliged entity (BYOD security).

1.10. Change Management Policy

a) Rules and procedures for change management.

b) Rules and procedures for identifying and approving changes that have or may have an impact on cybersecurity.

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

d) Rules and procedures for assessing the risks associated with a major change and selecting security measures.

e) Rules and procedures for managing significant change.

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 rollback.

h) Rules and procedures for deciding whether 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 respect to the use of the zero trust principle.

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

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

h) Software and Information Licensing and Acquisition Policy

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

2) rules and procedures for monitoring compliance with the licence conditions.

1.12. Access Control Policy

a) Policies and procedures for working with the Identity Management and Authentication tool and the tools for managing access permissions and defining the responsibilities of responsible persons.

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

c) The access control life cycle and the identification of those responsible for each phase.

d) The authorisation management lifecycle and the identification of those responsible for each phase.

e) Rules and procedures for managing privileged and administrator permissions.

f) Rules and procedures for emergency access control

g) Rules, procedures and records for accounts used primarily for recovery from a cybersecurity incident.

h) Regular review of access permissions, including the distribution of individual users in access groups.

i) Rules, procedures and requirements for access control of technical assets under management and technical assets outside the management of the obliged entity.

j) Rules for authentication mechanisms and password policies.

1.13. Cybersecurity event and incident management policy

a) Defining a cybersecurity event and a cybersecurity incident.

b) Rules and procedures for the continuous detection, recording and evaluation of cybersecurity events.

c) Rules and procedures for identifying and managing cybersecurity incidents

d) Policies and procedures for identifying, collecting, obtaining, and preserving credible evidence needed to analyze a cybersecurity incident.

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

f) Rules and procedures for reporting unusual behaviour of technical assets and suspected vulnerabilities.

g) Rules and procedures for evaluating, resolving, and determining the cause of cybersecurity incidents and for periodically updating the rules for evaluating cybersecurity incidents.

h) Cybersecurity incident reporting.

i) Records of cybersecurity 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 service 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 each service.

f) Escalation procedures for crisis situations.

g) Catalogue of crisis scenarios.

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

i) The method and period of testing of each business continuity plan and recovery plan.

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

1.15. Physical Security Policy

a) Determination of physical security perimeters and their levels.

b) Rules and procedures for the protection of each level of physical security perimeters.

1) Rules and procedures for the control and registration of entry of persons.

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

3) Rules and procedures for detecting physical security breaches.

1.16. Communication network security policy

a) Rules and procedures to ensure network segmentation and separation of environments.

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

c) Determination of rights and responsibilities for managing the secure operation of the communications network.

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

e) Rules and procedures for managing 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 the supplier or others.

1.17. Event logging policy

a) Defining the scope, the frequency of updating the scope of technical assets and the person responsible for keeping the scope up to date.

b) Rules and procedures for linking technical assets to an event log collection tool.

c) Rules and procedures for the unambiguous identification of technical assets to unambiguously identify the originator of a recorded event.

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

e) Rules and procedures for recording the activities of administrators, contractors and other privileged accounts.

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

g) Rules for retention of recorded events.

1.18. Policy on the deployment, use and maintenance of cybersecurity event detection tools and cybersecurity event collection and assessment tools

a) Rules and procedures for deploying tools to detect cybersecurity events.

b) Procedures and processes for detecting cybersecurity events from recorded events.

c) Policies, procedures and processes for evaluating and responding to detected cybersecurity events, including escalation procedures and contacts to relevant individuals.

d) Rules and procedures for optimizing the setup of tools designed to detect cybersecurity events.

e) Rules and procedures for optimally setting the security properties of a tool for collecting and evaluating cybersecurity events.

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

1.19. Vulnerability and patch management policy

a) Rules and procedures for limiting software installation.

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

c) Rules and procedures for the recording of technical assets not supported by the manufacturer, supplier or other person.

d) Rules and procedures for dealing with updates, patches and new versions of software and equipment and how to find them.

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

f) Policies and procedures for deploying updates, patches, and new versions of software and equipment, including procedures and processes for failover and rollback.

g) Rules and procedures for vulnerability scanning, working with findings and then retesting the finding.

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

1.20. Policy on the use of cryptography

a) Rules and procedures for the use of cryptographic algorithms, particularly in software and equipment and within a communications network.

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

c) Rules and procedures for cryptographic key and certificate management.

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

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 (in particular removable devices, disks, backup media).

1.21. Long-term storage, backup and recovery policy

a) Backup, recovery and retention requirements.

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

c) Rules and procedures for the connection and removal of technical assets within the backup system.

d) Backup rules and procedures.

e) Rules and procedures for restoring backups.

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

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

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

2. Contents of security documentation

2.1. Cybersecurity Audit Implementation Plan.

2.2. Cybersecurity audit report

a) Objectives of a cybersecurity audit.

b) Subject of the cybersecurity audit.

c) Cybersecurity audit criteria.

d) Identifying the audit team and the individuals who participated in the cybersecurity audit.

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

f) Findings from the cybersecurity audit.

g) Cybersecurity 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) non-conformities and corrective actions,

2) monitoring and measurement results,

3) audit results,

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

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

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

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

g) Identify opportunities for continuous improvement.

h) Recommending the necessary decisions, determining security measures and the persons responsible for carrying out the individual activities.

2.4. Methodology for asset identification and evaluation

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

1) determining a scale for assessing the confidentiality levels of assets,

2) determining a scale for assessing asset integrity levels,

3) determining a scale for assessing asset availability levels.

b) Determine a scale for evaluating supporting assets, taking into account the links between assets.

2.5. Methodology for risk identification and assessment

a) Determination of the risk assessment scale

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

2) determining a scale for assessing threat levels,

3) determining a scale for assessing vulnerability levels,

4) determining a scale for assessing risk levels.

b) Methods and approaches for risk management.

c) Methods of approving acceptable risks.

2.6. Asset and risk assessment report

a) Summary of the asset and risk assessment process.

2.7. Declaration of applicability

a) A summary of the security measures required by this Decree that have not been applied, including the reasons why they have not been applied.

b) An overview of the security measures applied, including how they were implemented.

2.8. Risk Management Plan

a) The objectives and benefits of the selected security measures for managing individual risks, including the link to specific risks.

b) Resources required for individual security measures to manage risks.

c) Persons responsible for enforcing individual security measures to manage risks.

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

e) Method of implementing security measures.

2.9. Security Awareness Development Plan

a) Content and timing of briefings to users, administrators, security role holders, contractors and senior management.

b) Content and dates of initial and regular training.

c) Summaries that include the subject matter of each training and a list of persons who have received the training.

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

2.10. Overview of generally binding legislation, internal regulations and other regulations and contractual obligations

a) Overview of generally binding legislation.

b) Overview of internal rules and regulations.

c) Overview of contractual obligations.

2.11. Methodology for carrying out the impact analysis

a) Methods for assessing the impact of cybersecurity incidents on continuity and assessing the associated risks.

2.12. Business continuity plans

a) Plan activation conditions.

b) Specification of the persons to be guided by the plan.

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

2.13. Recovery plans

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

b) A method of verifying successful data recovery from a 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) Description of these technical assets.

b) Guarantors of these technical assets.

c) Methods of implementing security measures to ensure a similar or higher level of security for these technical assets.

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

a) Description of these technical assets, accounts and authentication mechanisms

b) Justification for not introducing multi-factor authentication

2.16. Other recommended documentation

a) Infrastructure topology.

b) Infrastructure segmentation.

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

d) Links to the contact persons responsible for system and technical support.

Annex No. 6 to Decree No. XXXX Coll.
Cybersecurity Management Committee and security roles

This Annex contains a description of the recommended requirements for the Cybersecurity Management Committee and the security roles listed in § 5 and § 6.

Table 1: Cybersecurity Management Committee

Role:	**Cybersecurity Management Committee**
Key activities:	a) Responsibility for the overall management and development of cybersecurity within the obliged entity. b) Creation of a cybersecurity framework, direction and principles for the cybersecurity of the obliged entity (defining strategic objectives and guiding development in the field of cybersecurity). c) Definition of roles and responsibilities within the information security management system. d) Definition of reporting and control requirements for the information security management system. e) Reviewing the current status of cybersecurity within the obliged entity and determining whether planned objectives are being met.
Other conditions:	a) A member of the cybersecurity management committee shall be at least 1. a representative of the senior management or his/her delegate, 2. cybersecurity manager.

	b) The members of the Cybersecurity Management Committee shall meet regularly and the proceedings and outcomes of the meetings shall be maintained in paper or electronic form.

Table 2: Cybersecurity Manager

Role:	**Cybersecurity Manager**
Key activities:	a) Responsibility for the management of the information security management system. b) Regular reporting to the senior management of the obliged entity. c) Regular communication with the senior management of the obliged entity. d) Coordinating and participating in the asset and risk management process. e) Submission of asset and risk assessment reports, risk management plan and applicability statements to the Cybersecurity Management Committee. f) Providing guidance to ensure information security in the establishment, evaluation, selection, management and termination of contractor relationships g) Communication with Government or National CERT. h) Incident Management Coordination. i) Evaluating the appropriateness and effectiveness of security measures.
Knowledge:	a) 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 emphasis on security c) Risk management. d) Business continuity management. e) Relevant legal and regulatory requirements, in particular the law. f) Context of the obliged entity.
Experience:	a) Promoting an 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 information or cybersecurity, or b) graduation from a university and at least 1 year of experience in information or cybersecurity.
Relevant certifications*:	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 incompatible with roles responsible for the operation of the information and communication system and with other operational or management roles. b) The necessary authority, responsibility and budget must be secured for the proper performance of this role.

Table 3: Cybersecurity Architect

Role:	**Cybersecurity Architect**
Key activities:	a) Responsibility for the design of the implementation of security measures. b) Responsibility for establishing, documenting, maintaining and continually developing an appropriate secure architecture for the regulated service in accordance with current good practice
Knowledge:	a) Information and communication systems architecture 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) Security and risk management. f) Security of communications and networks. g) Identity and access control. h) Security evaluation and testing. i) Traffic security. j) Basic principles of secure software development. k) Integration and dependencies of ICT and business processes.
Experience:	a) Designing the implementation of security measures. b) Designing a security architecture with a focus on goals and security. c) Software development security.
Education and experience:	a) At least 3 years of experience in information or cybersecurity, or b) graduation from a university and at least 1 year of experience in information or cybersecurity.
Relevant certifications*:	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.

Table 4: Cybersecurity Auditor

Role:	**Cybersecurity Auditor**
Key activities:	a) Conducting a cybersecurity audit. b) Evaluation of the correctness and effectiveness of the security measures in place.
Knowledge:	a) Information security audit methodology and frameworks. b) Internal audit processes and procedures. c) The role and function of internal audit. d) ICT security audit process. e) Strategic and tactical ICT management. f) ICT acquisition, development and deployment. g) Management of ICT operations, maintenance and services. h) Asset protection. i) Cybersecurity assessment, testing and sampling methods. j) Relevant legislation. k) ICT security.

Experience:	a) Planning information or cybersecurity audits. b) Conducting cybersecurity audits or information security management system audits. c) Analysing the results of audits. d) Writing audit conclusions, presenting them and proposing recommendations to correct findings. e) Reporting on the status of compliance with legal requirements. f) Conducting audits with a focus on ICT and information or cybersecurity.
Education and experience:	a) At least 3 years of experience in information or cybersecurity auditing, or b) graduation from a university and at least 1 year of experience in the field of information or cybersecurity auditing.
Relevant certifications*:	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), Auditor BI (CIA accreditation scheme).
Other conditions:	a) Role incompatible with roles 1. the Cybersecurity Management Committee, 2. the cybersecurity manager, 3. the cybersecurity architect, 4. the asset guarantor. b) The role is incompatible with roles responsible for the operation of information and communication systems.

Table 5: Asset guarantor

Role:	**Asset guarantor**
Key activities:	a) Responsibility for ensuring the development, use and security of the asset. b) Cooperation with other persons in security roles. c) Performing asset and risk identification and assessment.
Knowledge:	a) Good knowledge of the asset of which he is the guarantor. b) Good knowledge of internal security policies and methodologies (e.g. Asset and Risk Assessment Methodology).

* Certification may be other than that specified if the certification attesting the competence of the security roles meets the requirements of ISO 17024.

Annex No. 7 to Decree No. XXXX Coll.
Supplier management - security measures for contractual relationships

Contents of contracts with major suppliers:

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

b) provisions on the authorisation to use data,

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

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

e) provisions governing the supply chain, ensuring that subcontractors undertake to comply fully with the arrangements between the obliged entity and the supplier and not to conflict with the obliged entity's requirements of the supplier,

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

g) change management provisions,

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

i) provisions on the supplier's obligation to inform the obliged entity of

   1. cybersecurity incidents related to the performance of the contract,
   2. the supplier's risk management arrangements and the residual risks associated with the performance of the contract,
   3. a significant change in control of that Supplier under the Corporations Act or a change in ownership of, or authority to dispose of, material assets used by that Supplier to perform under the contract with the Obliged entity,
   4. a request by a foreign authority for access to or transmission of data processed in the territory of a foreign State, except where such information would be contrary to the law under whose jurisdiction the data processing takes place or under which the request was made.

j) specification of conditions in terms of security at the end of the contract, the so-called exit strategy (for example, a transition period at the end of cooperation, when it is still necessary to maintain the service before deploying a new solution, data migration, etc.),

k) specification of the conditions for business continuity management in relation to suppliers (e.g. inclusion of suppliers in emergency plans, tasks of suppliers when activating business continuity management),

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

m) data disposal rules,

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

o) provisions on penalties for breach of obligations,

p) provisions on disclosure or transfer of data following a request by a foreign authority for disclosure or transfer of data processed in the territory of a foreign State

   1. only after a review of the legality of the application has been carried out,
   2. only after efforts have been made to prevent disclosure or transfer of the data within the limits of the law under which the processing takes place or under which the request was made,
   3. only to the extent necessary.

Annex No. 8 to Decree No. XXXX Coll.

Recommended topics for developing security awareness

a) Equipment security techniques
b) Firewall, antivirus and their limitations
c) Malicious programs and their manifestations
d) Risks of downloading programs and applications
e) Software updates
f) Risks of enabling/disabling macros
g) Risks of executables
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 working 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 behaviour of technical assets and suspected vulnerabilities
u) Basic procedure for responding to a cybersecurity event or incident
v) Policy on the use of work equipment for private purposes
w) Policy on the use of personal devices for work purposes (BYOD security)
x) Personal responsibility of the employee in complying with cybersecurity policies
y) Current threats in cybersecurity