Proposal

DECREE

dated dd.mm.yyyy,

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

The National Office for Cyber and Information Security shall determine pursuant to § 55(1)(c) and (d) of Act No. [to be added] Coll., on Cyber Security (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 regulates for the providers of regulated services in the regime of lower obligations (hereinafter referred to as the "obliged entity")

a) the content and scope of the security measures; and
b) how to determine the significance of the impact of a cyber security incident.

§ 2
Definition of terms

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

a) administrator is a privileged user or person who is responsible for the administration, operation, use, maintenance and security of a technical asset,
b) security policy is a set of principles and rules that determine how to ensure the protection of assets,
c) privileged user is an authority or person whose activities on a technical asset may have a significant impact on the security of a regulated service,
d) user is a natural or legal person or public authority using the asset,
e) top management means the person or group of persons who manage the obliged entity or the statutory body of the obliged entity,

[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) 20/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

f) ensuring cybersecurity means ensuring a minimum level of cybersecurity of the obliged entity's assets based on the implementation of security measures.

PART TWO

SECURITY MEASURES

§ 3

The obliged entity shall establish and implement security measures in accordance with this Decree within the scope of cyber security management established pursuant to § 13 of the Act.

§ 4

Ensuring cyber security

(1) The obliged entity shall establish and implement appropriate security measures taking into account the security needs of the organisation as part of ensuring cyber security. The obliged entity shall always establish and implement at least the security measures referred to in § 4 to § 6 and § 11.

(2) Obliged entity shall

a) prepare a summary of the security measures required by this Decree in accordance with Annex 1, which shall include at least

1. a summary of all security measures that have been implemented, including a description of their implementation,
2. a summary of all security measures to be implemented, including the dates for their implementation, the priority for their implementation, the identification of the person responsible for their implementation, and
3. a summary of any security measures that have not been implemented, including the reasons for not implementing them,

b) at least once a year, carry out and document an evaluation of the effectiveness of the security measures in place, including an update of the security measures overview,

c) store individual summaries of the security measures with which senior management is demonstrably familiar pursuant to § 5(c) for at least 4 years.

(3) The obliged entity shall designate a person responsible for cybersecurity who is responsible for managing and developing cybersecurity, overseeing the status of cybersecurity, and communicating cybersecurity to senior management; designated can be only a person which

a) without undue delay undergoes the training referred to in § 6 (g) or

b) demonstrates professional competence in cyber security.

(4) Obliged entity shall with regards to management of security policy and security documentation

a) establish and approve a security policy and maintain security documentation covering the areas listed in Annex 2 to this Decree,
b) update relevant security policies and security documentation.

(5) The obliged entity shall comply with the rules and procedures set out in the security policy and security documentation referred to in paragraph 4(a).

(6) In accordance with the identification and inventory of assets under the Act, the obliged entity shall establish and implement rules for the protection and permissible use of assets.

(7) When concluding contracts with suppliers, the obliged entity shall ensure that the contracts with these suppliers contain in particular the relevant areas listed in Annex 3 to this Decree.

(8) In connection with the planned acquisition, development, and maintenance of technical assets, the obliged entity shall establish and enforce cybersecurity security requirements, based in particular on the requirements for security measures under this Decree.

§ 5

Duties of top management

Top management with regards to ensuring cyber security

a) is demonstrably informed of its duties and the extent of its responsibilities,
b) ensure the availability of the resources needed to ensure cyber security in accordance with the security measures overview,
c) is demonstrably familiar with the implementation of the safety measures overview referred to in § 4(2)(a).

§ 6

Security of human resources

Obliged entity shall with regards to security of human resources

a) establish a policy on safe user behaviour, taking into account the relevant topics listed in Annex 4 to this Decree,
b) establish rules for the development of security awareness, including rules for the creation of passwords according to § 9,
c) conducts initial cyber security awareness training in accordance with the Security Awareness Development Policy,
d) conducts regular cyber security training in accordance with the Security Awareness Development Policy,
e) take into account the relevant topics listed in Annex 4 to this Decree in the training referred to in points (c) and (d),
f) keep records of the training referred to in points (c) and (d),

g) ensure the necessary theoretical and practical training of administrators and persons responsible for cyber security in accordance with their job description,
h) ensure compliance with the security policy; and
i) determine the rules and procedures for dealing with breaches of the rules laid down.

§ 7

Business continuity management

Obliged entity shall with regards to business continuity management

a) within the primary assets, establish their priority and the order and procedures for their renewal,
b) sets out the responsibilities and obligations for restoration under point (a),
c) 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 cyber security incident.

§ 8

Access control

(1) The obliged entity controls access to assets based on operational and security needs; with regards to access control it shall
   a) assign access rights and permissions and a unique identifier to each user and administrator accessing the technical assets,
   b) limit the assignment of administrator and privileged permissions to the level necessary to perform the job,
   c) control the identifiers, access rights and permissions of technical asset accounts,
   d) implement the security measures necessary for the safe use of mobile devices and other technical equipment, and, where appropriate, safety measures related to the use of technical equipment that the obliged entity does not have under its control,
   e) periodically review the settings of all access permissions,
   f) ensure that access permissions are removed or changed when users or administrators are reassigned or reassigned,
   g) ensure that access privileges are removed or changed when the contractual relationship is terminated or changed; and
   h) establishes the rules for the creation of passwords according to § 9.
(2) The obliged entity shall with regards to the physical security prevent unauthorised access to its assets and prevent damage, theft and unauthorised interference.

§ 9

Identity management and permissions

(1) The obliged entity shall use a tool to manage identities and their permissions to ensure
   a) managing access permissions,
   b) identity management,
   c) control the number of possible failed login attempts,
   d) re-verification of identity after a specified period of inactivity; and
   e) the robustness of the stored and transmitted authentication data.

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

(3) The obliged entity shall, until the use of an authentication mechanism based on multi-factor authentication pursuant to paragraph 2, use authentication by means of cryptographic keys or certificates.

(4) The obliged entity shall, until the use of an authentication mechanism using cryptographic keys or certificates as referred to in paragraph 3, use an authentication tool based on an account identifier and a password and this 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) to verify the identity of technical assets, the default password must be changed immediately and a new password must be created using a random string of upper and lower case letters, numbers and special characters,
   c) unrestricted use of lower and upper case letters, numbers and special characters,
   d) mandatory password changes at intervals of no more than 18 months,
   e) 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.

(5) The obliged entity shall also, in the context of identity management
   a) ensure that confidentiality is maintained when creating default authentication credentials and when restoring access; and
      1. ensure that the default password or password used to restore access is changed after the first use,
      2. invalidate the password or identifier used to restore access within 72 hours of its creation,
   b) ensure that the access password is changed without delay in the event of reasonable suspicion of its compromise; and

c) secure administrator accounts of technical assets used especially for recovery from a cybersecurity incident and use these accounts only when strictly necessary.

§ 10

Detection and logging of cyber security events

(1) As part of the detection of cyber security events, the obliged entity shall ensure
   a) verification and control of transmitted data at the perimeter of the communication network, including blocking unwanted communication,
   b) a tool for continuous and automatic protection against malicious code on individual relevant technical assets, in particular on
      1. servers,
      2. end stations,
   c) regular updates of detection tools and their rules,
   d) control of automatic content launching and
   e) continuous provision of information on relevant detected cyber security events and timely alerting of relevant persons.

(2) The obliged entity shall records cybersecurity events and relevant operational events in accordance with paragraph 1 and shall record in particular the following for those events
   a) date and time, including time zone specification,
   b) type of activity,
   c) a unique identification of the technical asset and account identification; and
   d) the success or failure of the activity.

§ 11

Cyber Security Incident Response

(1) Obliged entity in the context of dealing with cyber security events and incidents
   a) ensure that users, administrators, persons responsible for cybersecurity, other employees and contractors report unusual behaviour of technical assets and suspected vulnerabilities,
   b) develop a methodology for assessing cyber security events and cyber security incidents, including those with significant impact in accordance with § 15,
   c) ensure the assessment of cybersecurity events and cybersecurity incidents, including those with significant impact, in accordance with the methodology referred to in point (b),
   d) ensure the handling of cyber security incidents,
   e) report cyber security incidents with significant impact under § 16 of the Act,
   f) produce a final report on a cyber security incident with a significant impact under § 17 of the Act, including a description of the cause of the cyber security incident with a significant impact, if known.

(2) The obliged entity shall ensure the detection of cyber security events and shall furthermore use the tools referred to in § 10 in their detection.

§ 12

Security of communication networks

Obliged entity shall for the protection of the security of the communication network, in particular its network perimeter,

a) ensure the segmentation of the communication network, especially the separation of the operational and backup environments,
b) restrict outgoing and incoming communications at the perimeter of the communications network to those necessary for the proper provision of the regulated service,
c) uses currently resilient and secure network protocols,
d) in the case of the use of remote connection to the internal communication network or remote management of the technical assets of the regulated service
    1. limit these connections to those that are strictly necessary,
    2. implement security measures to ensure the confidentiality and integrity of these remote connections and remote management; and
    3. has an overview of the users and administrators who are using these remote connections or remote administration.

§ 13

Application security

Obliged entity shall for ensuring the safety of the regulated service

a) ensure that security updates issued for technical assets are applied without delay,
b) for technical assets that are no longer supported by the manufacturer, supplier or other person
    1. keep records of them,
    2. implement security measures to ensure a similar or higher level of safety; and
    3. limit their communication on the communication network to what is necessary,
c) performs vulnerability scans of relevant technical assets and applies appropriate security measures based on the results.

§ 14

Cryptographic algorithms

(1) Obliged entity for ensuring the protection of technical assets and their communication
    a) uses encryption using currently robust cryptographic algorithms where appropriate,
    b) promotes the secure handling of cryptographic algorithms and

c) takes 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 ensure safe

a) voice, audio-visual and text communication, including email communication and

b) emergency communication within the organisation.

PART THREE

METHOD FOR DETERMINING THE SIGNIFICANCE OF A CYBER SECURITY INCIDENT

§ 15

Determining the significance of the impact of a cyber security incident

(1) For the purposes of assessing the significance of the impact of a cyber security incident on the provision of a regulated service, the obliged entity shall determine

a) the tolerable level of harm caused by a cybersecurity incident, representing the aggregate of the highest damages and non-pecuniary damages arising from a cybersecurity incident that does not yet result in a threat to the life or health of persons or the ability of the regulated service provider to meet its obligations,

b) areas for assessing the significance of the impact of cyber security incidents on the organisation, taking into account

1. the operational impact of a cyber security incident on the obliged entity and its ability to provide a regulated service,
2. the number of employees, users of the regulated service and other bodies and persons affected by a cyber security incident,
3. the time and resources required to restore the provision of the affected regulated service,
4. the location of the incident defining the significance of the part of the assets affected by the cyber security incident for the provision of the regulated service,
5. the sensitivity of the data affected by the cybersecurity incident and the damage or non-pecuniary harm that a breach of the security of that data may cause to the obliged entity or to another authority or person,
6. the cause of the cybersecurity incident, if known to the obliged entity, in particular whether the proximate cause was human error, technical failure or intentional.

(2) The impact of a cybersecurity incident on the provision of a regulated service shall be considered significant if it exceeds the tolerable level of harm caused by the cybersecurity incident as determined by the obliged entity pursuant to paragraph 1 (a) and is also assessed as significant on the basis of the areas referred to in paragraph 1 (b).

PART FOUR
EFFECTIVENESS

§ 16
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.

Overview of security measures

Evaluation of the effectiveness of cybersecurity for the year					
Security measures required by the Decree	**Security measure status (implemented/ not implemented/ in the process of implementation)**	**Description of the security measure/ justification for not implementing the security measure**	**Planned date of implementation of the security measure**	**Priority for the introduction of a security measure**	**Person responsible for implementing the security measure**

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

Security policy and security documentation

1. Policy for ensuring a minimum level of cyber security
    a) The scope and boundaries of cybersecurity governance.
    b) Rules for protection and permissible uses of assets.
    c) The requirements of the service level agreement and the manner and level of implementation of security measures.
    d) Security requirements for acquisition, development and maintenance management.
2. Human Resources Security Policy
    a) Rules for the development of security awareness and the recording of training summaries.
    b) Safety training for new employees.
    c) Determining the period for regular training.
    d) Rules for dealing with breaches of security policy.
    e) Rules for termination of employment or change of position
        I. the return of assets entrusted to them and the withdrawal of rights on termination of the employment relationship,
        II. changing access permissions when changing job roles,
        III. handing over responsibilities when changing jobs or terminating employment with administrators or the person responsible for cyber security.
    f) Rules for secure user behaviour, including rules for creating passwords.
3. Business Continuity Management Policy
    a) Prioritization of primary assets and the sequence and procedures for their recovery, including assignment of responsibilities.
    b) Communication matrix with key persons for each service.
    c) Procedures for starting and stopping the system, for restarting or resuming the system after a failure, and for handling error conditions or abnormal events.
    d) Backup rules and procedures.
4. Access Control Policy
    a) Rules and procedures for managing privileged permissions.
    b) Rules, procedures and records for accounts used primarily for recovery from a cyber security incident.
    c) Rules for periodic review of access permissions, including the distribution of individual users in access groups.
5. Cyber Security Event Detection and Cyber Security Incident Response Policy
    a) Defining a cybersecurity event and a cybersecurity incident.
    b) Rules and procedures for the identification and classification of incidents of significant impact under Part Three of this Decree.
    c) Rules and procedures for reporting unusual behaviour of technical assets and suspected vulnerabilities.
    d) Reporting of cyber security incidents with significant impact.
6. Communication Network Security Policy
    a) Rules and procedures for managing remote access to the communications network, including remote access by contractors or others.
    b) Rules and procedures for remote management of technical assets, including remote management of technical assets by the supplier or others.

7. Application Security Policy
    a) Rules for regular updates.
    b) Rules for securing technical assets that are no longer supported.
    c) Vulnerability scanning rules.
8. Asset records
9. Overview of security measures
10. Recovery plans
11. Final report on a cyber security incident
12. Records of unsupported technical assets
13. Other recommended documentation
    a) Infrastructure topology.
    b) Infrastructure segmentation.
    c) Overview of technical assets, especially network devices, active elements, end devices and servers.
    d) Contacts for technical and system support.

Annex 3 to Decree No XX/XXXX Coll.

Requirements for contractual arrangements with suppliers

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

Contents of contracts with suppliers:

a) Provisions to ensure information security (requirement to ensure confidentiality, integrity and availability),
b) the supplier audit clause,
c) provisions on subcontracting,
d) provisions governing the so-called exit strategy, the conditions for terminating the contractual relationship from a security perspective,
e) provisions on penalties for breach of contractual obligations,
f) provisions on the authorisation to use data,
g) provisions on authorship of program code or program licenses,
h) the confidentiality provisions of the contractual relationship,
i) provisions governing the obligation to comply with the rules for supplier, which have been made demonstrably known to relevant supplier personnel,
j) change management provisions,
k) provisions on cyber security incidents related to the performance of the contract,
l) provisions governing business continuity management,
m) the details of the service level agreement (SLA) and the method and level of implementation of security measures.

The obliged entity is recommended to require, when concluding contracts with suppliers, additional arrangements taking into account specific requirements arising from the provision of operational and security needs related to the regulated service not listed in this Annex.

Annex No. 4 to Decree No. XX/XXXX Coll.

Recommended topics for developing security awareness

a) Device security techniques
b) Firewall, antivirus and their limitations
c) Malicious programs and their manifestations
d) Risks of downloading programs and apps
e) Software updates
f) Risks of enabling/disabling macros
g) Risks of executable files
h) User account security policy
i) Using, creating and managing passwords
j) Multi-factor authentication
k) Social engineering techniques
l) Online identity, digital footprint and its minimisation
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) Using cloud storage
t) Rules and procedures for reporting unusual behaviour of technical assets and suspected vulnerabilities of any kind
u) Basic procedure for responding to a cyber security 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) Employee's personal responsibility to comply with cyber security principles
y) Current threats in cyber security