UNIVERSITY OF PARDUBICE	
Directive No. 4/2026	
Subject:	Information Security Policy – Ensuring Cybersecurity at the University of Pardubice
Applicable to:	All organisational units of the University of Pardubice and its constituent parts, employees and students of the University of Pardubice
Effective Date:	26 March 2026
Reference Number:	UPCE/opo/00003291/2026
Prepared by:	Ing. Jiří Slanina, Cybersecurity Manager
Submitted by:	Ing. Olga Klápšťová, Director of CITS
Approved by:	doc. Ing. Liběna Černohorská, Ph.D., Vice-Rector for Internal Affairs

PART I
GENERAL PROVISIONS

Article 1
Introductory Provisions

The purpose of this Directive is to declare the intention of the University of Pardubice (UPCE) to implement and manage cybersecurity within UPCE and to establish the fundamental principles, rules, scope of cybersecurity management, and the boundaries for ensuring and maintaining cybersecurity.

This Directive is binding on all employees and students of UPCE. These persons are required to comply with the principles and rules set out in this Directive and its annexes.

Article 2
Subject Matter

1. This Directive, *Information Security Policy – Ensuring Cybersecurity at UPCE* (hereinafter the "Directive"), is issued pursuant to Act No. 264/2025 Sb., on Cybersecurity (hereinafter the "Act"), and its implementing legislation, in particular Decree No. 408/2025 Sb., on Regulated Services, Decree No. 409/2025 Sb., on Security Measures for Providers of Regulated Services under the Higher Obligations Regime, and Decree No. 334/2025 Sb., on the Portal of the National Cyber and Information Security Agency and Requirements for Certain Actions.

2. This Directive forms part of the information security policy within the Information Security Management System (ISMS) at UPCE.

3. This Directive defines, within UPCE, the composition of the Cybersecurity Management Committee (hereinafter the "Cybersecurity Management Committee") and the security

roles, their responsibilities, and their rights and obligations related to the Information Security Management System.

Article 3
Definitions of Key Terms

1. **Administrator** means a privileged user or another person responsible for the administration, operation, use, maintenance and security of a technical asset.

2. **Acceptable risk** means a risk that is acceptable to UPCE.

3. **Asset** means any physical or digital resource, document, person or activity related to the processing of information and data in electronic form.

4. **Information security** means the protection of confidentiality, integrity and availability of information and data.

5. **Security policy** means a set of principles and rules defining how assets are protected.

6. **Security roles in relation to assets:**
   a) **Primary asset owner** means a person or supervising officer of a unit who bears overall responsibility for a given primary asset in terms of its purpose, use and alignment with the objectives of UPCE,
   b) **Supporting asset owner** means a person or supervising officer of a unit who bears overall responsibility for a given supporting asset in terms of its purpose, significance and alignment with the needs of the assets it supports,
   c) **Asset owner** (hereinafter also the "Owner") means collectively the primary asset owner and the supporting asset owner,
   d) **Functional asset administrator** (hereinafter also the "Functional Administrator") means a professionally competent designated person or supervising officer of a unit responsible for the substantive and content accuracy of an asset, i.e. ensuring that the asset fulfils its purpose and meets the needs of users and processes at UPCE,
   e) **Technical administrator of a supporting asset** (hereinafter also the "Technical Administrator") means a professionally competent designated person or supervising officer of a unit responsible for the technical administration, operation and implementation of security measures of a given supporting asset,
   f) **User** means a natural or legal person or a public authority using UPCE assets,
   g) **Privileged user** means a user, person or administrator whose activities on a technical asset may have a significant impact on the security of a regulated service,
   h) **Natural person acting as user, author, originator or owner of information, document, record or file** means a specific identifiable person who:
      i. created the information, document, record or file (author, originator),
      ii. uses, modifies or administers it (user), or
      iii. otherwise mediated it or is responsible for its creation, content or retention,

i) **Other security roles** mean the Cybersecurity Management Committee, Cybersecurity Manager, Cybersecurity Architect and Cybersecurity Auditor.

7. **CIA** means the triad of cybersecurity principles defining the three primary objectives of information protection:
   C = Confidentiality – protection against unauthorised access
   I = Integrity – protection against unauthorised modification
   A = Availability – ensuring access to information when needed

8. **Data** means records of actions, facts or information and sets thereof, including operational data and metadata, particularly in the form of text, numbers, graphs, images, audio and video.

9. **Risk assessment** means the overall process of identifying, analysing and evaluating risks.

10. **Threat** means any potential circumstance, event or action that may cause a cybersecurity event or cybersecurity incident and may damage, disrupt or otherwise adversely affect assets, their users or other persons.

11. **Information** means processed, interpreted or organised data that carry meaning and context in electronic or paper form.

12. **CS** means cybersecurity.

13. **Cybersecurity event (hereinafter "CSE")** means an event that may result in a cybersecurity incident.

14. **Cybersecurity incident (hereinafter also "CSI")** means a disruption of information security in cyberspace.

15. **Cyberspace** means the environment consisting of electronic communications networks and other technologies in which information and data are processed in electronic form.

16. **Supporting asset** means an asset ensuring the functioning of primary assets or other supporting assets, in particular an employee, supplier, technical asset, building or other defined space where an asset of a regulated service is located.

17. **Primary asset** means an asset in the form of processed information or a provided service.

18. **Regulated service** means a registered service so designated by the National Cyber and Information Security Agency pursuant to Section 6(2) of the Act.

19. **Risk** means the possibility that a threat will exploit a vulnerability of an asset and cause damage.

20. **Risk management** means a systematic process including risk assessment, implementation of security measures to address risks, and risk communication.

21. **Information Security Management System (ISMS)** means the part of the UPCE management system based on a risk approach to assets, defining how information security is established, implemented, operated, monitored, reviewed, maintained and improved.

22. **Technical asset** means a technical or software resource or equipment.

23. **Top management** means the Rector, Vice-Rectors and the Bursar.

24. **Research and development** means the conduct of applied research aimed at the commercial use of its results. This includes:
    a) **Sensitive research activity**, meaning applied research concerning military material listed under the Act on Foreign Trade in Military Material,
    b) **Applied technology research**, meaning activities falling within technological areas defined by the European Commission as critical for the EU's economic security.

25. **Significant threat** means a threat which, based on its technical characteristics, can be expected to have the potential to seriously affect the assets of a regulated service provider or its users to such an extent that it causes substantial harm.

26. **Significant supplier** means an entity providing services or deliverables to a regulated service provider that are significant from the perspective of cybersecurity.

27. **Significant change** means a change that has or may have an impact on cybersecurity and involves a significant risk.

28. **Ensuring cybersecurity** means ensuring a minimum level of cybersecurity of the obliged entity's assets based on the implementation of security measures.

29. **Vulnerability** means a weakness of an asset or a security measure that may be exploited by a threat.

30. **Cybersecurity incident handling** means activities aimed at prevention, detection, analysis, impact mitigation, response and recovery.

Article 4
UPCE as a Provider of Regulated Services and the Regime Applicable to Regulated Service Providers; Notification and Registration of Regulated Services

1. Based on the criteria for identifying regulated services pursuant to Section 4(1)(a) and (b) of the Act, and Annex to Decree No. 408/2025 Sb., on Regulated Services, UPCE is a provider of regulated services listed in Annex No. 1 to this Directive.

2. In relation to the regulated services identified in Annex No. 1 to this Directive, UPCE meets the criteria of a regulated service provider subject to the higher obligations regime.

3. UPCE, as a provider of regulated services, declares that it has fulfilled the conditions for the notification and registration of these services pursuant to Section 6 of the Act and, for the purposes of the decision on registration of regulated services, has notified the National Cyber and Information Security Agency (hereinafter the "Agency") via its portal within the time limit set by the Act.

4. Changes to the regime of a regulated service provider and the cancellation of the registration of a regulated service shall be governed by the Act.

Article 5
Obligations of UPCE as a Provider of Regulated Services

1. As a provider of regulated services, UPCE shall, no later than 30 days from the delivery of the Agency's decision on the registration of a regulated service, notify the Agency of:
   a) contact details (first name and surname of the authorised or designated person, their role or position in relation to the regulated service provider, their telephone number and email address) of natural persons authorised to act on its behalf in matters governed by the Act, and, where applicable,
   b) additional information, including details of its ownership structure, technical data relating to the regulated service, and information on its geographical scope and cross-border provision.

2. UPCE, as a provider of regulated services, shall report changes only to those data that are not reference data maintained in basic registers, no later than 14 days from the date on which such changes occurred.

PART II
CYBERSECURITY MANAGEMENT

Article 6
Determination of the Scope of Cybersecurity Management

1. The scope of cybersecurity management at UPCE (hereinafter the "defined scope") includes assets related to the provision of regulated services.

2. For the purpose of defining the scope, UPCE has:
   a) identified all its primary assets,
   b) assessed whether the primary assets are related to the provision of regulated services, and
   c) for the primary assets referred to in point (b), identified the supporting assets.

3. UPCE maintains records of assets included in the defined scope and of primary assets excluded from the defined scope, including the reasons for their exclusion.

4. Primary assets that have not yet been assessed under paragraph 2(b) and supporting assets that have not yet been identified under paragraph 2(c) shall be considered part of the defined scope.

5. UPCE, as a provider of regulated services, shall regularly review (at least once per year) and update the defined scope.

Article 7
Security Measures

1. Security measures are organisational and technical measures aimed at ensuring the proper provision of regulated services and the cybersecurity of assets by UPCE.

2. Within the defined scope, UPCE, as a provider of regulated services, shall implement and apply the security measures listed in paragraph 5 of this Article to the extent necessary to ensure the cybersecurity of regulated services. UPCE shall commence the implementation and application of security measures for each regulated service no later than one year from the date of delivery of the decision on its registration.

3. Where UPCE implements or applies security measures through a supplier, it shall select the supplier in accordance with the requirements arising from the relevant security measure and incorporate such requirements into contracts with the supplier.

4. The content of security measures and the manner of their implementation and application are specified by the Agency in Decree No. 409/2025 Sb., on Security Measures for Providers of Regulated Services under the Higher Obligations Regime.

5. For UPCE as a provider of regulated services under the higher obligations regime:

a) <u>organisational measures include</u>:

1. Information Security Management System,
2. requirements for top management,
3. definition of security roles,
4. management of security policy and security documentation,
5. asset management,
6. risk management,
7. supplier management,
8. human resources security,
9. change management,
10. acquisition, development and maintenance,
11. access management,
12. handling of cybersecurity events and incidents,
13. business continuity management, and
14. cybersecurity auditing,

b) <u>technical measures include</u>:

1. physical security,
2. security of communication networks,
3. identity management and authentication,
4. access rights and permissions management,
5. detection of cybersecurity events,
6. event logging,
7. evaluation of cybersecurity events,
8. application security,
9. cryptographic algorithms,
10. ensuring the availability of regulated services, and
11. security of industrial, control and other specific technical assets.

6. In ensuring cybersecurity, UPCE shall follow its security policy and security documentation, in particular:

a) it has established and approved a relevant security policy in accordance with paragraph 5(a) and (b) and maintains corresponding security documentation,

b) it regularly reviews the security policy and security documentation and ensures that they remain up to date,

c) it complies with and enforces compliance with the rules and procedures set out in the security policy and security documentation pursuant to Section 6 of Decree No. 409/2025 Sb., on Security Measures for Providers of Regulated Services under the Higher Obligations Regime.

Article 8
Reporting and Procedure for Reporting Cybersecurity Incidents

1. UPCE, as a provider of regulated services under the higher obligations regime, specifically the Cybersecurity Manager, shall report cybersecurity incidents (CSI) to the Agency that have occurred within the defined scope, originate in cyberspace, and where intentional causation cannot be excluded within 24 hours of detection. The Cybersecurity Manager shall submit an initial notification no later than 24 hours after detection of the CSI, including identification details, basic information about the CSI, and an indication of whether the CSI is believed to have been caused by unlawful interference or may have cross-border impact.

2. Upon request of the Agency, the Cybersecurity Manager shall provide the necessary information and cooperation in handling the CSI, where the intended purpose cannot be achieved otherwise or would be significantly hindered. Such cooperation need not be provided where prevented by statutory or state-recognised confidentiality obligations or by the performance of another legal obligation.

3. The Cybersecurity Manager shall maintain records of CSIs, cybersecurity events (CSEs), threats and vulnerabilities.

4. Where a CSI has a significant impact on the national cyberspace, the Cybersecurity Manager shall additionally submit:
   a) without undue delay, and no later than 72 hours after detection of the CSI, a notification updating the information provided under paragraph 1, including an initial assessment of the CSI and, where available, its impact and indicators of compromise,
   b) upon request of the Agency or the National CERT, an interim report on significant developments in the handling of the CSI, and
   c) no later than 30 days from the submission of the notification under point (a), a final report on the resolution of the CSI; where the CSI persists beyond this period, the Cybersecurity Manager shall submit, without undue delay after the expiry of the period, an interim report on the current status of handling the CSI, followed by a final report no later than 30 days after the CSI has been resolved.

5. The Cybersecurity Manager shall report CSIs, including voluntary reports, via the Agency's Portal. Where the Portal cannot be used, the Cybersecurity Manager shall submit the report via the Agency's designated email address for CSI reporting or via its data mailbox.

Article 9
Handling of CSIs at UPCE and Information Obligation

1. The Agency shall provide its statement on the CSI without undue delay, and no later than 24 hours after receipt of the initial notification from the Cybersecurity Manager.

2. Upon request of the Cybersecurity Manager, the Agency shall provide methodological support for the implementation of mitigation measures and, where appropriate, further technical support for handling the reported CSI.

3. The Cybersecurity Manager shall, upon request of the Agency, provide the necessary information and cooperation in handling the CSI, where the intended purpose cannot be achieved otherwise or would be significantly hindered. Such cooperation need not be provided where prevented by statutory or state-recognised confidentiality obligations or by the performance of another legal obligation.

4. Where the Cybersecurity Manager considers it appropriate, for the purpose of ensuring the proper provision of regulated services and the cybersecurity of assets, they shall, without undue delay, inform users of the regulated service of any CSI with a significant impact that may adversely affect the provision of that service. The Agency may impose an obligation or prohibition on UPCE to inform users of the regulated service about such an incident.

Article 10
Countermeasures

1. Countermeasures are actions taken by the Agency necessary to protect assets against threats, exploitation of vulnerabilities in the field of cybersecurity, or against CSIs, or to address an ongoing CSI.

2. Countermeasures include:
   a) alert,
   b) warning, and
   c) reactive countermeasures.

3. Definitions of individual countermeasures are set out in the relevant provisions of the Act.

Article 11
Final Provisions

1. Directive No. 7/2021, *Basic Information Security Policy – Ensuring Cybersecurity at the University of Pardubice*, is hereby repealed.

2. This Directive shall enter into force and take effect on the date of the Rector’s signature.

In Pardubice, 26 March 2026

prof. Ing. Libor Čapek, Ph.D.
Rector

Annexes:

1. List of regulated services provided by UPCE and applicable regime
2. List of primary assets of UPCE
3. Information Security Management System Policy (ISMS)
4. Policy on Requirements for Top Management; Statute of the Cybersecurity Management Committee; Rules of Procedure of the Cybersecurity Management Committee
5. Security Roles Policy
    - Statute of the Cybersecurity Manager
    - Statute of the Cybersecurity Architect
    - Statute of the Cybersecurity Auditor
    - Designation of Persons Responsible for Assets
    - Statute of the Asset Owner
    - Statute of the Functional Administrator
    - Statute of the Technical Administrator

Policy for the Management of Security Policy and Security Documentation

List of Regulated Services Provided by UPCE and Applicable Regime

1. Based on the criteria for identifying regulated services pursuant to Section 4(1)(a) and (b) of the Act, and Annex to Decree No. 408/2025 Sb., on Regulated Services, UPCE is a **provider of the following regulated services**:

   - **under the higher obligations regime:**
   a) No. 19, point 19.1(a) Science, Research and Education – Research and Development,
   b) No. 21, point 21.1 Defence Industry – Manufacture of Military Material listed under the Act on Foreign Trade in Military Material,
   c) No. 21, point 21.2 Defence Industry – Trade in Military Material under the Act on Foreign Trade in Military Material.

2. UPCE further provides the following regulated service:
   a) No. 1.1 Exercise of Conferred Powers,
   which corresponds to the lower obligations regime; however, UPCE meets the criteria of a regulated service provider subject to the higher obligations regime.

List of Primary Assets of UPCE

1. Primary assets of UPCE are defined based on the list of regulated services identified at UPCE pursuant to the Act and the relevant legal regulations.

2. Primary assets represent actual activities and processes carried out at UPCE in the performance of its conferred powers, the provision of education, the conduct of scientific, research, development, innovation and related activities, as well as internal management and administration of the University. They are aligned with the mission, strategic objectives and legal obligations of UPCE.

3. From the perspective of the Act, primary assets have a dual nature in terms of cybersecurity:
   - **service-related nature** – representing the provision of activities, functions or the exercise of powers towards internal or external entities,
   - **information-related nature** – inherently linked to the processing, storage or transmission of information and data in electronic form.

4. Accordingly, these primary assets are treated in two aspects:
   - as a **service of UPCE**, for which availability and continuity must be ensured,
   - as **information of UPCE**, for which availability, integrity and confidentiality must be ensured.

   Their protection and management are carried out through supporting assets, organisational measures and security mechanisms in accordance with this Directive.

5. For each primary asset listed below, a primary asset owner from among UPCE senior management is designated.

No.	Primary Asset	Primary Asset Owner
1	Exercise of Conferred Powers	Vice-Rector for Education and Quality
2	Educational Activities	Vice-Rector for Education and Quality
3	Scientific, Research and Creative Activities	Vice-Rector for Research and Creative Activities
4	Research and Development in the Defence Industry	Vice-Rector for Research and Creative Activities
5	Manufacture of Military Material	Rector
6	Trade in Military Material	Rector
7	Internal and Strategic Management	Vice-Rector for Internal Affairs
8	Internal Administration	Bursar
9	External Relations	Vice-Rector for External Relations

Information Security Management System Policy (ISMS)

1. The definition of the ISMS scope is subject to approval by the Cybersecurity Management Committee and must include all primary assets ensuring the provision of regulated services operated at UPCE.

2. The implementation of the ISMS constitutes a key organisational security measure for ensuring the proper provision of regulated services and the cybersecurity of assets.

3. Within the Information Security Management System, UPCE has established the following ISMS objectives:
   a) to ensure and implement appropriate security measures aimed at ensuring the cybersecurity of regulated services and minimising the impact of cybersecurity incidents on their provision,
   b) to ensure the capability to restore regulated services following a cybersecurity incident or other extraordinary event,
   c) to ensure the protection of information processed in the provision of regulated services against unauthorised access and modification,
   d) to ensure that access to information systems and information is managed according to job roles and the principle of need-to-know,
   e) to systematically identify, assess and manage cybersecurity risks affecting regulated services and their supporting assets in accordance with Decree No. 409/2025 Sb., on Security Measures for Providers of Regulated Services under the Higher Obligations Regime,
   f) to define and approve security policies and security documentation related to cybersecurity management, including an exception management process,
   g) to establish an effective process for detection, reporting, analysis and handling of cybersecurity incidents,
   h) to increase awareness among employees and students of cybersecurity and their responsibilities when handling information,
   i) to ensure regular evaluation of the effectiveness of the ISMS through an ISMS review report submitted to the Cybersecurity Management Committee and UPCE management,
   j) to ensure the performance of cybersecurity audits,
   k) to update the ISMS based on audit findings, risk assessments, incident impacts and changes in relevant legislation.

4. In implementing the ISMS, UPCE shall ensure compliance with the basic obligations set out in Section 3 of Decree No. 409/2025 Sb., on Security Measures for Providers of Regulated Services under the Higher Obligations Regime.

Policy on Requirements for Top Management; Statute of the Cybersecurity Management Committee; Rules of Procedure of the Cybersecurity Management Committee

Part I
Hierarchy of Security Roles in Relation to UPCE Assets

1. The hierarchy is designed to enable coordination of ISMS activities within UPCE through individuals representing security roles.

Figure 1: Hierarchy of Security Roles in Relation to Primary Assets

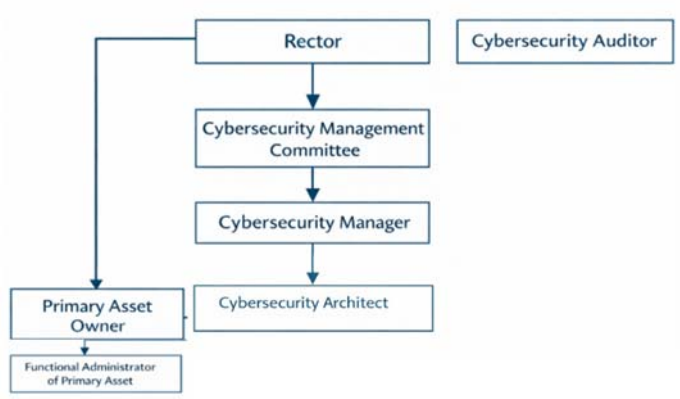
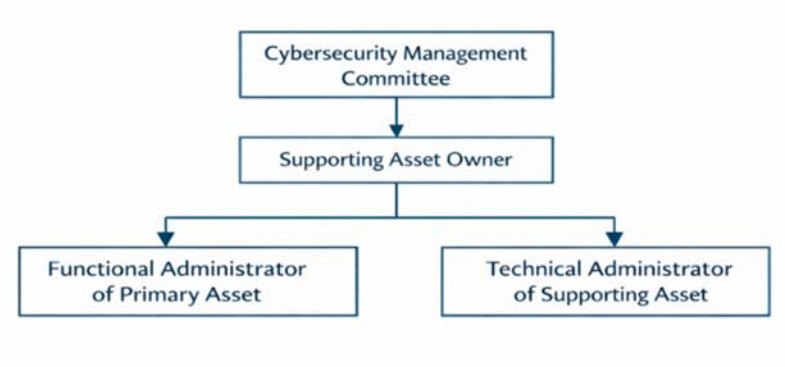


Figure 2: Hierarchy of Security Roles in Relation to Supporting Assets



Part II
Policy on Requirements for Top Management

1. The management of UPCE recognises the importance of ensuring cybersecurity and commits to creating conditions enabling the achievement of the objectives set out below.

2. The objectives of UPCE management include:
   a) ensuring training of top management regarding its responsibilities and the security policy, particularly in the areas of the ISMS, risk management and business continuity management, through initial and regular training aimed at acquiring knowledge and skills necessary for identifying risks and assessing the appropriateness of selected risk management approaches and their impact on regulated services,
   b) ensuring the establishment of the security policy and ISMS objectives aligned with the strategic direction of UPCE,
   c) ensuring the integration of the ISMS into UPCE processes,
   d) ensuring sufficient financial resources for the ISMS,
   e) informing employees about the importance of the ISMS and the importance of achieving compliance with its requirements among all relevant stakeholders,
   f) ensuring support for achieving ISMS objectives,
   g) supporting and guiding employees in improving the effectiveness of the ISMS,
   h) participating in the development of business impact analysis,
   i) ensuring the testing of business continuity plans, recovery plans and processes related to the handling of cybersecurity incidents,
   j) promoting continuous improvement of the ISMS,
   k) supporting persons performing security roles in promoting cybersecurity within their areas of responsibility,
   l) ensuring the establishment of rules for the designation of administrators and persons performing security roles,
   m) ensuring confidentiality is maintained by all users (in particular administrators, persons performing security roles and suppliers),
   n) ensuring that persons performing security roles are granted the authority necessary to fulfil their roles, as well as resources, including budgetary resources, required for the performance of their roles and related tasks.

3. UPCE management demonstrably familiarises itself with:
   a) the ISMS review report,
   b) the risk assessment report,
   c) the results of the business impact analysis, and
   d) the results of cybersecurity audits and cybersecurity inspections.

Part III
Statute of the Cybersecurity Management Committee

Article 1
Introductory Provisions

1. The Cybersecurity Management Committee is established by decision of the Rector to ensure the overall management and development of the Information Security Management System within the meaning of the Act and its implementing legislation.

2. This Statute of the Cybersecurity Management Committee defines the basic scope of its competence, membership, organisational arrangements for its meetings, decision-making procedures, and outputs of its activities.

Article 2
Composition of the Cybersecurity Management Committee

1. The Cybersecurity Management Committee consists of five members appointed and approved by the Rector.

2. The members of the Cybersecurity Management Committee are:
   a) Vice-Rector for Internal Affairs – Chair of the Cybersecurity Management Committee,
   b) Bursar – Deputy Chair of the Cybersecurity Management Committee,
   c) Cybersecurity Manager,
   d) Director of the Centre for Information Technology and Services,
   e) an academic staff member of UPCE with relevant expertise in the overall management and development of the system for ensuring minimum cybersecurity, appointed by the Rector upon proposal of the Academic Senate of UPCE for the duration of the Rector's term of office.

3. The Rector, the Data Protection Officer and the Secretary of the Cybersecurity Management Committee shall attend meetings of the Committee as permanent invitees without voting rights; the role of the Secretary is defined in Article 5 of this Annex.

4. Membership of the Chair and/or Deputy Chair in the Cybersecurity Management Committee shall terminate upon expiry of the Rector's term of office, dismissal, or resignation.

5. Membership of the other members of the Cybersecurity Management Committee shall terminate upon their dismissal, following a proposal by the Rector and prior discussion within the Committee, or upon their resignation.

Article 3
Activities of the Cybersecurity Management Committee

1. The Cybersecurity Management Committee shall in particular:

a) be responsible for the overall management and development of cybersecurity within UPCE,
b) be responsible for establishing the cybersecurity framework, strategic direction and principles of cybersecurity at UPCE (including defining strategic objectives and development priorities),
c) define the rights, duties and responsibilities of individual security roles within the ISMS,
d) define reporting requirements and oversight of the ISMS,
e) monitor the current state of cybersecurity within UPCE and assess whether planned objectives are being achieved,
f) review audit reports issued and approved by the Cybersecurity Auditor and reports on testing and evaluation of the effectiveness of implemented technical and organisational security measures.

2. The Cybersecurity Management Committee shall further review and submit to the Rector:
   a) assessments of the acceptability or unacceptability of identified cybersecurity risks, including the determination of acceptable risk levels,
   b) proposals for the allocation of financial resources for cybersecurity, submitted to the Committee by the Cybersecurity Manager,
   c) proposals for prioritising the implementation of individual security measures and cybersecurity projects submitted by the Cybersecurity Manager.

3. The Cybersecurity Management Committee shall review and submit to the Rector binding cybersecurity documentation, in particular:
   a) ISMS security policies,
   b) a list of information and communication systems included in the ISMS,
   c) ISMS review reports (at least once per year),
   d) the Risk Analysis and Risk Treatment Plan (at least once per year),
   e) minutes of the meetings of the Cybersecurity Management Committee or, where a CSI is identified, a report on the state of cybersecurity at UPCE.

4. In the area of personal data protection[1], the Cybersecurity Management Committee shall have the following powers and responsibilities:
   a) cooperate with the Data Protection Officer, who is a permanent invitee to the Committee, and take due account of their opinions,
   b) provide opinions on proposals and implementation of security processes for personal data protection within the scope of cybersecurity measures,
   c) inform the top management of UPCE about measures in the area of personal data protection within the scope of cybersecurity measures,
   d) in cooperation with the Data Protection Officer, assess the acceptability or unacceptability of identified personal data protection risks, including determining

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; Data Protection Act).

acceptable risk levels, taking into account the opinion of the Data Protection Officer,

e) submit proposals for the allocation of financial resources in the area of personal data protection within the scope of cybersecurity measures.

Article 4
Rights and Duties of Members of the Cybersecurity Management Committee

1. Members of the Cybersecurity Management Committee have the right to actively participate in its activities, raise questions, proposals and comments on reports and proposals under discussion, and express their views on addressing cybersecurity-related issues.

2. Members of the Cybersecurity Management Committee are required to attend its meetings and perform tasks assigned to them by the Committee.

3. The Chair of the Cybersecurity Management Committee shall in particular:
   a) direct and organise the activities of the Committee,
   b) issue opinions, recommendations and other documents of the Committee,
   c) assign tasks, based on decisions of the Committee, to persons responsible for cybersecurity and coordinate their implementation in order to ensure compliance of UPCE information and communication systems with legal regulations, internal regulations and UPCE standards.

4. Based on the Committee's deliberations, the Chair shall submit approved draft documents and proposals for expenditure from UPCE financial resources necessary to ensure the required level of cybersecurity to the top management of UPCE.

5. In the absence of the Chair, their duties shall be performed by the Deputy Chair.

Article 5
Administration of the Cybersecurity Management Committee

1. Administrative support for the activities of the Cybersecurity Management Committee shall be provided by the Secretary of the Committee.

2. The Secretary of the Cybersecurity Management Committee shall be an employee of UPCE appointed by the Chair of the Committee.

3. The Secretary of the Cybersecurity Management Committee shall:
   a) ensure organisational, technical and administrative support for the activities of the Committee,
   b) prepare draft agendas for Committee meetings,
   c) be responsible for the preparation and timely submission of supporting documents to Committee members in accordance with the Chair's instructions,
   d) prepare regular information on the activities of the Committee,
   e) maintain records (minutes, decisions) of meetings in paper or electronic form.

Article 6
Meetings of the Cybersecurity Management Committee

1. Meetings of the Cybersecurity Management Committee shall be convened as necessary, including extraordinary meetings, by the Secretary at the instruction of the Chair, but at least once every three months.

2. The Chair shall organise the work of the Committee and ensure the implementation of its resolutions. In the absence of the Chair or where urgent matters must be addressed, meetings shall be convened by the Deputy Chair.

3. The agenda of Committee meetings shall be proposed by the Chair, based on materials submitted for discussion, proposals from Committee members and tasks assigned at previous meetings.

4. Supporting materials for meetings shall be prepared primarily by the members of the Committee.

5. The collection and distribution of materials for Committee meetings shall be organised by the Secretary.

6. Meetings of the Cybersecurity Management Committee shall be governed by the Rules of Procedure of the Cybersecurity Management Committee.

Part IV
Rules of Procedure of the Cybersecurity Management Committee

Article 1
Introductory Provisions

The Rules of Procedure of the Cybersecurity Management Committee (hereinafter the "Rules of Procedure") govern its proceedings.

Article 2
Convening Meetings of the Cybersecurity Management Committee

1. Meetings of the Cybersecurity Management Committee shall be convened by the Secretary at the instruction of the Chair at least once every three months. Any member of the Committee may submit a written proposal to convene a meeting through the Secretary; the Chair shall decide on convening the Committee within five working days and schedule the meeting at the nearest appropriate date. In the event of an extraordinary security situation, the Chair may convene an extraordinary meeting immediately.

2. Members of the Cybersecurity Management Committee, permanent invitees and, where applicable, invited participants shall be invited to meetings, as a rule, at least five working days in advance.

3. Meetings of the Cybersecurity Management Committee may be held:
   a) in person,
   b) remotely using appropriate communication tools enabling secure transmission of audio and video and real-time communication.

4. The form of the meeting shall be decided by the Chair of the Cybersecurity Management Committee.

Article 3
Conduct of Meetings and Decision-Making

1. Meetings of the Cybersecurity Management Committee shall normally be chaired by the Chair, who may delegate this role to the Deputy Chair or another member of the Committee. The Committee shall adopt decisions in the form of resolutions, which must be recorded verbatim in the minutes.

2. The Cybersecurity Management Committee shall generally deliberate on the basis of written materials prepared in advance and submitted by its members.

3. The Committee shall consider materials in the order set out in the agenda approved at the beginning of the meeting.

4. Consideration of each item shall typically include an introductory presentation by the submitting party, questions and proposals from participants, and the adoption of a resolution.

5. The Cybersecurity Management Committee shall have a quorum if a majority of all its members are present.

6. Decisions shall be adopted by vote in the form of resolutions; adoption requires a majority of all members of the Cybersecurity Management Committee.

7. The Secretary shall prepare written resolutions and minutes of the meeting and distribute them to all participants.

8. Meetings of the Cybersecurity Management Committee shall not be public.

9. The Chair shall submit reports to the top management that the Committee is required to provide under the ISMS or whose submission is stipulated in adopted resolutions.

Article 4
Decision-Making *per rollam*

1. In exceptional cases between meetings, where materials cannot be submitted in the standard manner, the Chair may, upon a written request from the submitting party submitted via the Secretary, decide to approve materials *per rollam* using electronic communication.

2. Materials submitted for *per rollam* approval shall be distributed by the Secretary to all members of the Cybersecurity Management Committee, including information on the submitting party and a fixed deadline for submitting opinions (approval/disapproval), which shall be three working days unless specified otherwise. Members shall send their responses directly to the Secretary. Failure to respond within the specified deadline shall be deemed as a vote against. Upon receipt of responses, the Secretary shall evaluate them and distribute the final decision to all members. A proposal shall be deemed approved if a majority of all members express their approval within the specified deadline.

3. A resolution adopted in this manner shall have the same validity as a resolution adopted at a meeting of the Cybersecurity Management Committee.

4. At the next meeting, the Deputy Chair or a designated member shall inform the Committee of all resolutions adopted *per rollam* between meetings.

Article 5
Preparation and Submission of Materials

1. Materials for meetings of the Cybersecurity Management Committee shall be submitted to the Secretary at least two working days prior to the scheduled meeting, unless it is an extraordinary meeting, in which case materials may be submitted during the meeting.

2. Materials shall be submitted to the Secretary either in written form (one hard copy) or in electronic form.

Security Roles Policy

Part I
Statute of the Cybersecurity Manager

Article 1
Position of the Cybersecurity Manager

1. The role of the Cybersecurity Manager is established to ensure and perform cybersecurity functions at UPCE.
2. The Cybersecurity Manager reports directly to the Rector of UPCE.
3. The Cybersecurity Manager is appointed by the Rector of UPCE.
4. The Cybersecurity Manager performs duties arising from the role in accordance with the Act and its implementing legislation.
5. The Cybersecurity Manager shall not be assigned roles responsible for the operation of technical assets of regulated services. The role of the Cybersecurity Manager is incompatible with roles responsible for ICT operations (information and communication technologies) and with other operational and managerial roles.
6. The Rector shall ensure the substitutability of the Cybersecurity Manager. In the event of the long-term absence of the Cybersecurity Manager, the Rector shall appoint another suitable employee to act as a temporary replacement.

Article 2
Rights and Duties of the Cybersecurity Manager

1. The Cybersecurity Manager is responsible for:
   a) the registration of regulated services pursuant to Section 4 of the Act, including changes to and cancellation of such registration,
   b) maintaining the asset register of UPCE,
   c) managing the ISMS from initial assessments and analyses through ongoing preventive testing to the mitigation of consequences and evaluation of cybersecurity incidents at UPCE,
   d) regular reporting to the top management of UPCE on:
      - activities within their scope of responsibility,
      - the status of the ISMS,
   e) regular communication with the top management of UPCE,
   f) coordinating and participating in asset and risk management processes; continuously analysing developments in the ISMS and evaluating identified

cybersecurity risks, detected cybersecurity events (CSEs) and identified cybersecurity incidents (CSIs), and submitting reports thereon, including proposals for mitigating unacceptable risks and proposals for reprioritising cybersecurity projects to the Cybersecurity Management Committee,

g) submitting asset and risk assessment reports, the Risk Treatment Plan and the Statement of Applicability to the Cybersecurity Management Committee at least once per year,
h) providing guidance for ensuring information security in the establishment, evaluation, selection, management and termination of supplier relationships,
i) communication with the Government or National CERT,
j) coordinating the management of cybersecurity incidents,
k) evaluating the suitability and effectiveness of security measures.

2. The Cybersecurity Manager is authorised to define:
   a) a) the scope and boundaries of the cybersecurity management system (with regard to assets and organisational security), specifying which organisational units and technical components are included,
   b) a unified methodology for asset identification and assessment and criteria for risk acceptability,
   c) the objectives and strategy (plan) for business continuity management in the area of cybersecurity,
   d) operational rules and procedures of the cybersecurity management system,
   e) the Risk Treatment Plan, including the objectives and benefits of security measures and designation of persons responsible for their implementation.

3. The Cybersecurity Manager participates in the approval of binding internal regulations of UPCE concerning the selection, standardisation and systematisation of technical and software ICT resources.

4. In the implementation of new information systems that may affect cybersecurity at UPCE, the Cybersecurity Manager shall:
   a) provide assistance upon request,
   b) be informed of testing, pilot operation and stress testing,
   c) participate in the preparation of contractual documentation.

5. The Cybersecurity Manager reviews, from a substantive perspective, the formulation of procurement requirements (including low-value public contracts) for the development and modernisation of UPCE information and communication systems or for the acquisition of supplies or services whose components may affect cybersecurity, ensuring compliance with cybersecurity standards and providing assistance to contracting authorities in procurement procedures.

6. The Cybersecurity Manager decides on the implementation of security measures based on information from monitoring systems, decisions of the Cybersecurity Management Committee or decisions of the Agency.

7. The Cybersecurity Manager ensures in particular:
   a) detection of cybersecurity events, management of cybersecurity events and incidents, and decisions on their handling,
   b) preparation of asset and risk assessment reports and the Statement of Applicability, including an overview of implemented security measures,
   c) regular risk assessments of suppliers, verification of implemented security measures in provided services and remediation of identified deficiencies,
   d) updating the cybersecurity management system and related documentation based on audit results, significant changes and evaluation of the effectiveness of security measures,
   e) updating asset and risk assessment reports, security policies, the Risk Treatment Plan and the security awareness development plan,
   f) implementation of reactive measures issued by the Agency,
   g) cooperation during audits conducted by the Agency.

8. The Cybersecurity Manager proposes changes to the cybersecurity strategy of UPCE and to the ISMS security policy.

9. The Cybersecurity Manager prepares a security awareness development plan and presents it to the Cybersecurity Management Committee.

10. The Cybersecurity Manager coordinates measures to increase cybersecurity awareness at UPCE, including training and exercises, and defines rules for suppliers reflecting ISMS requirements.

11. The Cybersecurity Manager is authorised to request:
   a) from the Cybersecurity Management Committee:
      - decisions on the acceptability or unacceptability of identified cybersecurity risks, including acceptable risk levels and financial limits for mitigating unacceptable risks,
      - designation of persons to perform asset owner roles,
      - initial identification of assets,
   b) from the asset owner:
      - documentation for recording operating and recovery conditions of assets,
      - lists of current threats, vulnerabilities and identified risks,
      - assessment of risk acceptability,
      - methods for ensuring security parameters (levels) through Service Level Agreements (SLA),
      - identification of related supporting assets and their risks,
      - evaluation of the effectiveness of security measures.

12. In the event of a breach of established security policies and rules by a UPCE employee, the relevant supervising officer, in cooperation with the Cybersecurity Manager, shall duly investigate all circumstances and causes, assess the specific impact on the security situation, adopt effective measures to prevent recurrence, and ensure enforcement of any damages and sanctions against the responsible person. A similar procedure shall apply to external natural and legal persons.

Part II
Statute of the Cybersecurity Architect

Article 1
Position of the Cybersecurity Architect

1. The Cybersecurity Architect performs their role in accordance with the Act and its implementing legislation and is responsible for fulfilling tasks within the scope of the assigned security role.
2. The Cybersecurity Architect is proposed by the Cybersecurity Manager and appointed by the Rector of UPCE.
3. The role of the Cybersecurity Architect is incompatible with roles responsible for ICT operations.
4. The Rector shall ensure appropriate cover for the role of the Cybersecurity Architect. In the event of the long-term absence of the Cybersecurity Architect, the Rector shall appoint another suitable employee to act as a temporary replacement.

Article 2
Responsibilities and Powers of the Cybersecurity Architect

1. The Cybersecurity Architect is responsible for:
   a) ensuring the design of the implementation of security measures so as to achieve a secure architecture of regulated services,
   b) defining, documenting, maintaining and continuously developing an appropriate secure architecture of regulated services in line with current best practice, including assessing compliance of proposed security measures with legal requirements, technical and industry standards, and the strategy and needs of UPCE.

2. The primary role of the Cybersecurity Architect is, on the basis of the approved cybersecurity strategy and objectives of UPCE's security policy, to design and methodologically oversee the implementation of appropriate security measures at UPCE and to continuously analyse existing measures, reporting the results to the Cybersecurity Manager and the Cybersecurity Management Committee.

3. The Cybersecurity Architect independently ensures:
   a) the design and implementation of processes for the assessment and registration of assets and cybersecurity risks based on inputs provided by asset owners and the Cybersecurity Manager,

b) identification of appropriate approaches to achieving the required level of cybersecurity in accordance with the UPCE strategy,
c) the cybersecurity and information security architecture model of UPCE (including process model, application architecture, technologies, etc.),
d) identification of possible approaches and measures to reduce identified risks in accordance with the cybersecurity strategy and architecture, asset characteristics, environment and risks,
e) representation of UPCE in projects implementing cybersecurity measures, ensuring alignment with the cybersecurity architecture, asset characteristics, environment and risks,
f) in cooperation with other security roles:
   - contributing to the development of internal regulations and standards of UPCE in the area of information and cybersecurity,
   - contributing to the creation and updating of the catalogue of threats and vulnerabilities of UPCE assets,
   - contributing to the updating of the cybersecurity strategy and planning in line with strategic objectives of UPCE,
   - contributing to the definition of key projects for implementing the security policy and achieving the target cybersecurity architecture model,
   - supporting the implementation of new processes, including organisational arrangements and transition to new operating models in information and cybersecurity,
   - ensuring implementation oversight of selected cybersecurity measures and their integration within the cybersecurity architecture of UPCE,
   - cooperating in processes related to handling cybersecurity events (CSEs) and cybersecurity incidents (CSIs).

Part III
Statute of the Cybersecurity Auditor

Article 1
Position of the Cybersecurity Auditor

1. The Cybersecurity Auditor performs the security role as designated by the Rector in accordance with the Act, its implementing legislation and the principles of internal audit.

2. The role of the Cybersecurity Auditor is incompatible with membership of the Cybersecurity Management Committee and with other security roles. It is also incompatible with roles responsible for ICT operations and is performed independently.

3. The primary role of the Cybersecurity Auditor is to conduct cybersecurity audits at UPCE, ensuring that such audits are carried out impartially.

Article 2
Responsibilities and Powers of the Cybersecurity Auditor

1. The Cybersecurity Auditor is responsible for fulfilling tasks within the scope of the assigned security role, in particular:
   a) conducting cybersecurity audits,
   b) evaluating the correctness and effectiveness of implemented security measures.

2. The Cybersecurity Auditor has the right to:
   a) access and obtain information necessary for the performance of audits within the defined scope,
   b) participate in defining measures to address findings identified during audits,
   c) contribute to the development and refinement of methodologies for cybersecurity audits.

3. The Cybersecurity Auditor is obliged to:
   a) plan cybersecurity audits of UPCE information and communication systems in accordance with the principles of internal audit,
   b) maintain audit documentation in accordance with the principles of internal audit,
   c) prepare final audit reports for individual cybersecurity audits and submit them, together with proposed corrective measures, to the Cybersecurity Management Committee, the Cybersecurity Manager and the primary asset owner of the audited system. The Cybersecurity Management Committee shall review the audit report and decide on the implementation plan for the proposed corrective measures.

Part IV
Designation of Persons Responsible for Assets

1. The process of designating persons responsible for assets is designed to ensure clear accountability for asset management, separation of functional and technical responsibilities, and effective oversight of the security and operation of assets throughout their lifecycle. Relationships between individual roles are based on the principles of accountability, professional independence and mutual cooperation.

2. The designation of responsible persons depends on the specific type of asset, with clearly defined responsibilities and roles for each type of asset in accordance with this Directive.

Figure 3: Designation of Persons Responsible for Primary Assets

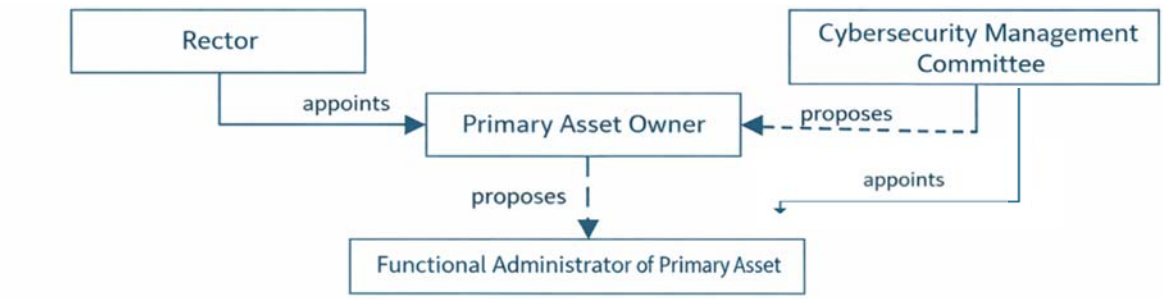
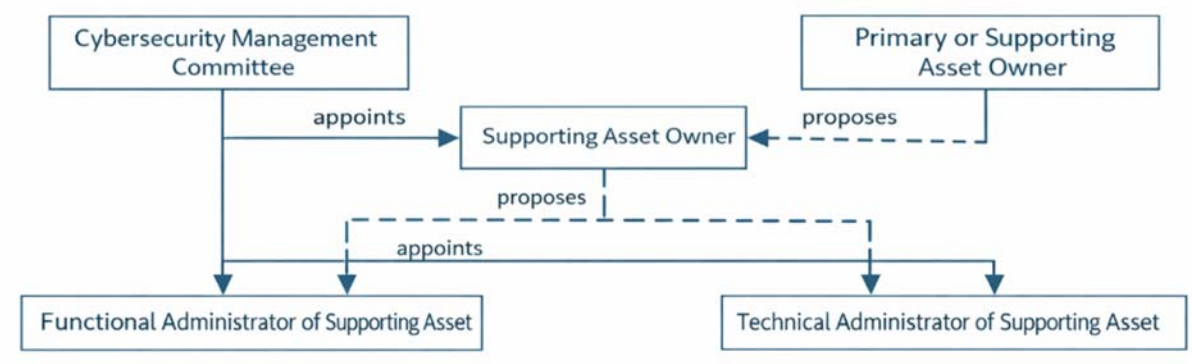


Figure 4: Designation of Persons Responsible for Supporting Assets



Part V
Statute of the Asset Owner

Article 1
Position of the Asset Owner

1. The Asset Owner is responsible for ensuring the development, use and security of the asset.

2. The Asset Owner is a security role with the most comprehensive overview of how the asset and the information it contains are managed in terms of processes and information management. For the performance of this role, the Asset Owner must be thoroughly familiar with UPCE processes.

3. The Asset Owner performs their role in accordance with the Act and its implementing legislation and is responsible for fulfilling tasks within the scope of the assigned security role.

4. The Primary Asset Owner is proposed by the Cybersecurity Management Committee and appointed by the Rector of UPCE.

5. The Supporting Asset Owner is proposed by the Primary Asset Owner or another Supporting Asset Owner and appointed by the Cybersecurity Management Committee.

6. The Primary Asset Owner is authorised to propose a person for the role of Functional Administrator of the primary asset. The role of Technical Administrator is not defined for primary assets, as it is not relevant.

7. The Supporting Asset Owner is authorised to propose persons for the roles of Functional Administrator and Technical Administrator of the supporting asset.

8. The Asset Owner cooperates with and directs persons in the roles of Functional Administrator and Technical Administrator and cooperates with other persons performing security roles.

9. The Primary Asset Owner does not directly administer the asset. Their role is to receive inputs in the areas of risk management, change management, planned outages and other processes that may affect the primary asset. They also propose extensions or changes to the purpose of the asset and provide other security roles with a description of the asset to ensure the quality of UPCE processes supported by the asset.

10. The Primary Asset Owner acts as the representative of the primary asset in strategic decision-making of UPCE management and during audits.

Article 2
Responsibilities and Powers of the Asset Owner

1. The Primary Asset Owner is responsible for ensuring that the asset is properly managed, protected and developed. They define its purpose, significance and strategic objectives, particularly in relation to the mission of UPCE, legal obligations and regulated services provided.

2. The Supporting Asset Owner is responsible for ensuring that the supporting asset is aligned with the requirements of the owners of the assets it supports. They define its purpose, significance and usage strategy so that it effectively and securely supports one or more assets.

3. The Asset Owner has the following responsibilities and powers:
   a) ensuring the development, use and security of the assigned asset,
   b) fulfilling ISMS requirements related to the assigned asset in accordance with legal regulations and internal rules, particularly in the area of organisational measures and processes supported by the asset,
   c) deciding on changes to the asset in terms of functionality, security and risks, including its decommissioning or replacement,
   d) determining asset classification, maintaining a list of supported processes and assessing other parameters,
   e) approving asset security documentation,
   f) participating, in the area of security documentation, in the identification and assessment of risks related to the asset and its supporting assets and submitting proposals to the Cybersecurity Manager regarding the acceptability or unacceptability of identified cybersecurity risks and corrective measures,
   g) cooperating with the Cybersecurity Manager in handling cybersecurity events (CSEs) and incidents (CSIs), including implementation of reactive measures in accordance with instructions of the Cybersecurity Manager or the Cybersecurity Management Committee,
   h) providing advance notice of planned outages or modifications of the assigned asset.

4. The Asset Owner is authorised to:
   a) request from the Functional Administrator and Technical Administrator:
      - all necessary information on the status of the asset, updated assessments of threats, vulnerabilities, risks, and recovery and continuity plans,
      - ensuring completeness of the asset and verifying that it meets defined requirements,
   b) suspend the use of the asset in the event of significant risks,
   c) be informed of decisions of the Cybersecurity Management Committee concerning the assigned asset, particularly in cases where the Committee does not approve the Asset Owner's proposed assessment of risk acceptability,

d) request final audit reports concerning the assigned asset from the Cybersecurity Auditor,
e) submit a request to the Chair of the Cybersecurity Management Committee to initiate an audit or inspection of related assets in case of suspected non-compliance.

Part VI
Statute of the Functional Administrator

Article 1
Position of the Functional Administrator

1. The Functional Administrator (of a primary or supporting asset) is proposed by the Asset Owner and appointed by the Cybersecurity Management Committee.
2. The Functional Administrator is an expert in the functional, process and content aspects of the asset.
3. The Functional Administrator is accountable to the Asset Owner. In the case of a supporting asset, their position is equivalent to that of the Technical Administrator.
4. The Functional Administrator ensures that the functional and process requirements defined by the Asset Owner are met.
5. The Functional Administrator plays a key role in assessing the impact of changes to the asset on its functionality and on the information provided by the asset.
6. The Functional Administrator cooperates with other persons performing security roles at UPCE.

Article 2
Responsibilities and Powers of the Functional Administrator

1. The Functional Administrator is responsible for:
   a) the substantive and content accuracy of the asset, ensuring that it fulfils its function and meets the requirements of the Asset Owner as well as the needs of users and UPCE processes,
   b) proposing functional and security requirements,
   c) assessing and evaluating risks from the perspective of operational and process impacts,
   d) providing expert support to the Asset Owner and the Technical Administrator in risk mitigation,
   e) informing the Asset Owner about access scopes and the use of the asset,
   f) cooperating with the Technical Administrator in assessing vulnerabilities, threats, incident handling and changes,
   g) maintaining and updating:
      - the functional description of the asset (purpose, functions, supported processes, relationships, content),
      - records of changes to the asset,
   h) reporting irregular or abnormal behaviour of the asset to the Asset Owner and the Cybersecurity Manager for the purpose of detecting cybersecurity events (CSEs) and cybersecurity incidents (CSIs),
   i) participating in audits and inspections.

2. The Functional Administrator is authorised to:
   a) propose functional and process changes to the asset,

b) request from the Technical Administrator technical information necessary for assessing the condition of the asset and updating recovery and continuity plans,
c) initiate the resolution of functional inconsistencies or risks,
d) assess proposals for technical changes from the perspective of functionality and content.

Part VII
Statute of the Technical Administrator

Article 1
Position of the Technical Administrator

1. The Technical Administrator is proposed by the Supporting Asset Owner and appointed by the Cybersecurity Management Committee.
2. The Technical Administrator is an expert in the operational and technical aspects of the asset.
3. The Technical Administrator is accountable to the Asset Owner, and their position is equivalent to that of the Functional Administrator.
4. The Technical Administrator ensures compliance with the functional, process and security requirements of the Asset Owner.
5. The Technical Administrator cooperates with other persons performing security roles at UPCE.

Article 2
Responsibilities and Powers of the Technical Administrator

1. The Technical Administrator is responsible for:
   a) technical administration, support and implementation of security measures for the asset,
   b) operation, availability, integrity, monitoring, maintenance and technical security of the asset,
   c) access management, logging, backup, updates, configuration, and functional and security testing in accordance with the requirements of asset owners and applicable standards,
   d) maintaining and updating:
      - recovery and continuity plans of the asset,
      - technical documentation, records of changes to the asset and recovery tests,
      - a list of services provided by the asset and required for its operation,
      - records of vulnerabilities and threats in accordance with Annex No. 3 to Decree No. 409/2025 Sb. as a basis for risk analysis, updated at least once per year,
   e) providing documentation, technical data and records to the Asset Owner and the Functional Administrator,
   f) reporting irregular or abnormal technical behaviour of the asset to the Asset Owner and the Cybersecurity Manager for the purpose of detecting cybersecurity events (CSEs) and cybersecurity incidents (CSIs),
   g) participating in audits and security inspections.

2. The Technical Administrator is authorised to:
   a) carry out technical interventions and configurations to ensure asset security in accordance with the requirements of the Asset Owner,
   b) propose technical security measures and improvements,

c) temporarily restrict the operation of the asset for the necessary period in the event of technical or security risks or during updates (subject to prior notification of the Asset Owner and the Functional Administrator),
d) request additional functional or organisational information from the Asset Owner or the Functional Administrator.

Policy for the Management of Security Policy and Security Documentation

1. Within the management of security policy and security documentation, UPCE shall:
   a) establish a security policy in relation to cybersecurity management and maintain relevant security policy and documentation for the measures set out in Sections 3–27 of Decree No. 409/2025 Sb., on Security Measures for Providers of Regulated Services under the Higher Obligations Regime,
   b) comply with the rules and procedures defined in the security policy and security documentation referred to in point (a),
   c) regularly review the security policy and security documentation, ensure they are kept up to date and reflect relevant aspects in operational rules, procedures and other documentation.

2. The Cybersecurity Manager is responsible for the regular review, update and alignment of the security policy and security documentation with operational documentation.

3. Security policy and security documentation shall be subject to approval by the Cybersecurity Management Committee.

4. Security documentation shall include, in particular, relevant parts of this Directive, the ISMS scope definition, dedicated security documentation for each regulated service, security policies and ISMS audit reports.

5. Security documentation shall be reviewed regularly (at least once per year); reviews may also be carried out on an ad hoc basis following audit findings or as a result of significant changes in UPCE's security requirements (e.g. changes in legislation or internal processes).

6. Security policy and security documentation shall be managed so as to ensure that they are:
   a) available in electronic or paper form,
   b) communicated within UPCE,
   c) appropriately accessible to relevant stakeholders,
   d) protected in terms of confidentiality, integrity and availability,
   e) maintained in a manner ensuring that the information contained therein is complete, legible, accurate, easily identifiable and retrievable.

7. The Cybersecurity Manager is responsible for ensuring the availability and proper placement of the current security policy and security documentation.