




Ensuring Cyber Security of Prague University of Economics and Business

Annotation:

In order to ensure a unified Information Security Management System (hereinafter referred to as "SŘBI") and the related supervision of its compliance within Prague University of Economics and Business, when implementing and complying with the requirements of Act No. 181/2014 Coll., on Cyber Security and Change of Related Acts (The Act on Cyber Security) and its implementing legislation or in direct connection with them, the roles of the Cyber Security Manager and the Cyber Security Committee of Prague University of Economics and Business are established.

	Processor:	Reviewed by:	Approved by:
Name:	Ing. Milan Nidl, MBA	-	Prof. Ing. Hana Machková, CSc.
Department / function:	Director Informatics Centre	-	Rector
Date:	April 27, 2021		April 27, 2021
Signature:	Ing. Milan Nidl, MBA m.p.	-	Prof. Ing. Hana Machková, CSc. m.p.
Validity from:	May 1, 2021	Validity until:	further notice
Effective from:	May 1, 2021	Effective until:	further notice

	Ensuring Cyber Security of Prague University of Economics and Business Directive No. 06/2021	Page 2 of 10 Document status 0
---	---	-----------------------------------

1. Recitals

- a) Prague University of Economics and Business, as part of the fulfillment of legal obligations to ensure cyber security (hereinafter referred to as "KB"), shall create the Information Security Management System (SŘBI)
- based on the standards principles of ČSN ISO/IEC 27001;
 - in accordance with the requirements for the security of important information systems according to the requirements of Act No. 181/2014 Coll., on Cyber Security and Change of Related Acts (The Act on Cyber Security);
 - and in accordance with the requirements for the security of personal data according to Directive No. 5/2018, Protection and Processing of Personal Data.
- b) The creation of the functioning SŘBI, including ensuring supervision of its functioning and the establishment of a related security policy and other security documentation, is a long-term process.

Cyber Security Committee of Prague University of Economics and Business


The Cyber Security Committee of Prague University of Economics and Business (hereinafter referred to as the "KB Committee") is hereby established as an advisory body to the Rector. The composition of the KB Committee, its rights and obligations are regulated in the Statutes of the KB Committee; the Statutes of the KB Committee form Annex 1 to this Directive.

2. Cyber Security Manager of Prague University of Economics and Business

The security role of the Cyber Security Manager of Prague University of Economics and Business is hereby established (hereinafter referred to as "KB Manager"). The activities of the KB Manager are governed by the Statutes of KB Manager, which form Annex 2 to this Directive.

Annexes to this Regulation:

- Annex No.1 - Statutes of the Cyber Security Committee of VŠE
- Annex No. 2 - Statutes of the Cyber Security Manager of VŠE.

	Ensuring Cyber Security of Prague University of Economics and Business Directive No. 06/2021	Page 3 of 10 Document status 0
---	---	-----------------------------------

Annex No. 1

Statutes of the Cyber Security Committee of VŠE

1. Recitals

1. Cyber Security Committee of Prague University of Economics and Business (hereinafter referred to as "KB Committee") is established to ensure:
 - cyber security management within the meaning of standards of ČSN ISO/IEC 27001 – Information Security Management System
 - cyber security management of important information systems pursuant to Act No. 181/2014 Coll., on Cyber Security and Change of Related Acts (The Act on Cyber Security), as amended (hereinafter referred to as "ZoKB") and its implementing legislation, in particular Decree No. 82/2018 Coll., on Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (hereinafter referred to as "VoKB").
 - data and information protection management within the meaning of standards of ISO/IEC 27701 – Privacy Information Management System.
2. The Statutes of the KB Committee set out the basic scope of its competence, membership of the KB Committee and the organizational arrangements for its conduct.

2. Activities of KB Committee

1. In particular, the KB Committee shall:
 - a) propose the objectives and strategy of cyber security of Prague University of Economics and Business (hereinafter referred to as "VŠE") and coordinate the preparation, implementation and development of the unified Information Security Management System of VŠE in the field of cyber security (hereinafter referred to as "SRBI");
 - b) discuss and recommend changes to the Security Policy and other cyber security documentation and controls the implementation of changes within VŠE;
 - c) approve the evaluation of the effectiveness of security measures, their consequences and suitability, as well as the identification of their corresponding alternatives suitable for VŠE,

- d) discuss audit reports, issued and approved by Auditor of Cyber Security of VŠE;
- e) inform the management of VŠE about cyber security measures;
2. The KB Committee shall further discuss and submit to the management of VŠE:
 - a) assessment of acceptability or unacceptability of identified cyber security risks, including determination of acceptable risk level;
 - b) proposals for the allocation of cyber security resources,
 - c) proposals to determine the order of importance of implementing individual security measures and security projects.
3. The KB Committee shall discuss and submit binding cyber security documentation to the management of VŠE, in particular:
 - a) the policy of the Information Security Management System;
 - b) documentation of the Information Security Management System (plan for the creation and updating of the SŘBI documentation);
 - c) a list of primary and secondary assets;
 - d) reports of the review of the SŘBI;
 - e) a declaration of applicability of the SŘBI;
4. The KB Committee shall submit a report on the state of cyber security of VŠE at least once a year.
5. In the area of protection of personal data¹, the KB Committee has following powers and responsibilities:
 - a) commenting on the design and implementation of security processes for the protection of personal data;
 - b) informing the management of VŠE about measures in the field of personal data protection;
 - c) submission of a proposal for the allocation of funds in the field of personal data protection.

3. Composition of the KB Committee

1. Membership of the KB Committee is determined by the position, the representative of the academic community is appointed and removed by the Rector.
2. Composition of the KB Committee:
 - Director of the Informatics Centre - Chairman of the KB Committee;
 - Bursar - Vice-Chairman of the KB Committee;

¹ within the meaning of Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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, GDPR).



- Cyber Security Manager
- Commissioner for Personal Data Protection of VŠE;
- a representative of the academic community;
- head of the department that is in charge of the operation of the study information system (InSIS).

4. Rights and Obligations of Members of KB Committee

1. The members of the KB Committee shall be obliged to participate in its deliberations and to carry out the tasks assigned to them by the KB Committee.
2. The Chairman of the KB Committee shall
 - a) manage and organize the work of the KB Committee;
 - b) decide to convene the KB Committee meeting in due and extraordinary time;
 - c) impose, on the basis of the decision of the KB Committee, tasks in the field of cyber security and coordinate their implementation in order to achieve the compliance of the information and communication systems of VŠE with the requirements of the ZoKB and internal legislation of VŠE;
 - d) monitor the implementation of the KB Committee resolution;
 - e) submit, on the basis of the meeting of the KB Committee, to the management of VŠE documents or requirements for the implementation of expenditures from the financial resources of VŠE.
3. In the absence of the Chairman of the KB Committee, the Vice-Chairman of the KB Committee shall carry out his/her duties.

5. KB Committee Meeting

1. The meetings of the KB Committee shall be convened:
 - regularly in due time;
 - furthermore, as appropriate, on the instructions of the Chairman of the KB Committee;
2. The Chairman shall also organize the work of the KB Committee and ensure the implementation of the KB Committee's resolutions is adopted. In the absence of the Chairman or the need to discuss or resolve urgent matters, the Vice-Chairman of the KB Committee shall convene the meeting.
3. The agenda of the KB Committee is proposed by the Chairman of the KB Committee. It is based on the documents submitted for discussion, the proposals of the members of the KB Committee and the tasks assigned to its deliberations.
4. The members of the KB Committee, in particular, prepare the expert documents for the KB Committee's deliberations.
5. The KB Committee shall be capable of acting if an above-half majority of all its members are present.
6. The KB Committee shall be decided by an overwhelming majority of its members.




The votes of the members of the KB Committee are equally valid.

7. The Chairman may invite guests to the individual points of the programme. However, they always have only an advisory capacity.
8. The minutes of the KB Committee's deliberations shall be drawn up in writing and signed by the chair of the KB Committee.
9. The administration of the activities of the KB Committee shall be ensured by the Secretary of the Committee, appointed by the Chairman of the KB Committee, who shall manage the Secretary's work.
10. The chair of the KB Committee may decide, where justified, that the KB Committee's deliberations shall take place using technical means

6. KB Committee Working Teams

To discuss factual topics, the KB Committee may set up expert working groups (teams) and appoint their heads, who will be composed of members of the KB Committee, representatives of the relevant departments of VŠE and invited external experts.

	Ensuring Cyber Security of Prague University of Economics and Business Directive No. 06/2021	Page 7 of 10 Document status 0
---	---	-----------------------------------


Annex No. 2

Statutes of the Cyber Security Manager of VŠE

Article 1

Cyber Security Manager of VŠE

- 1) The Cyber Security Manager of Prague University of Economics and Business (hereinafter as "KB Manager").
 - a) is appointed and removed by the Rector.
 - b) is responsible for managing the Information Security Management System (hereinafter referred to as "SŘBI") from research and analysis, through continuous environmental testing, prevention activities to elimination of consequences and evaluation of "successful" cyber incidents at VŠE.
 - c) is an authorized person communicating on behalf of VŠE with the National Cyber and Information Security Agency (hereinafter referred to as "NÚKIB") in the case of:
 - dealing with cyber security cases and incidents;
 - receiving reports from the NÚKIB on security situation and security threats;
 - coordination of the measures taken under the NÚKIB recommendation or regulation;
 - d) is an authorized person communicating on behalf of VŠE with the National Computer Emergency Response Team (hereinafter referred to as "Government CERT") for the coordination of measures in the information systems of VŠE.
 - e) is responsible for coordinating the implementation of cyber security projects approved by the Cyber Security Committee of VŠE (hereinafter only referred to as "KB Committee").
 - f) is responsible for providing professional methodological assistance to faculties and departments of VŠE in the field of cyber security.
 - g) is responsible for providing opinions to faculties and departments of VŠE and statements in the field of cyber security.

	<p>Ensuring Cyber Security of Prague University of Economics and Business</p> <p>Directive No. 06/2021</p>	<p>Page 8 of 10 Document status 0</p>
---	---	---

Article 2

Powers and Responsibilities of KB Manager

1) The KB Manager has the following powers:

- a) to continuously analyze the development of the SŘBI and evaluate identified cyber risks, detected cyber security cases and detected cyber incidents, for which the KB Manager presents a report including proposals to mitigate unacceptable risks and proposals to change the priorities of security projects, which he/she regularly submits to the KB Committee (see responsibilities);
- b) He/she is entitled to propose:
 - the scope and boundaries of the SŘBI (with regard to assets and organizational security), in which the he/she determines which organizational parts and technical elements are relevant to the SŘBI;
 - a single methodology for identifying and evaluating assets and a methodology for establishing criteria for risk acceptance;
 - business continuity objectives and a strategy (plan) to manage the continuity of further cyber security activities;
 - other parts of the security policy and security documentation;
 - SW and HW standards of components, systems, applications and functionalities of information and cyber security, including their configuration standards when set up in the project and in routine operation.
 - catalogue of information and cyber security services based on rules and standards (SLA, KPI, HW/SW standard) in accordance with applicable law.
 - a risk management plan containing the objectives and benefits of security measures for risk management, including the identification of persons responsible for implementing security measures;
 - concepts of recovery plans, business continuity objectives and other rules, including standardization of recovery processes after incidents and accidents.
- c) He/she is entitled to cooperate on the approval of binding standards for the selection, unification and systemization of technical and program resources of information technologies of VŠE;
- d) in the case of projects relating to information systems, he/she is entitled to:
 - consult the organization of checks on the stages of sub-implementation of projects;
 - decide with the IS operator to organize security testing in order to demonstrate the functionality of safety components and systems;
 - participate in the trial and verification operations;

- reject project takeover if the project does not meet security metrics.
- e) to control the formulation of procurement requirements for the construction and modernization of information and communication systems of VŠE in terms of cyber security standards;
- f) to factually check the formulation of the rules of delegated responsibilities to suppliers of ICT components, systems and services that take into account the needs of the SŘBI in order to balance penalty restrictions and SLA metrics in their application in case of any disruption of the operation or safety of the VŠE supplier.
- g) to propose changes to the cyber security strategy of VŠE and security policy;
- h) to coordinate security awareness measures, including cyber security training and practice.
- i) He/she is entitled to require:
 - I) from the guarantors of primary assets, processing and submission of:
 - the purpose of the asset and the conditions for its operation;
 - identified threats, vulnerabilities and risks to the asset;
 - an assessment of the acceptability of these risks;
 - the establishment of requirements for availability, confidentiality and integrity;
 - II) from the guarantors of secondary assets and administrators, processing and submission of:
 - identifying threats, vulnerabilities and risks to the asset;
 - an assessment of the acceptability of these risks;
 - evaluation of the effectiveness of the cyber security measures.

2) The KB Manager has the following responsibilities:

- a) development, enforcement and updating of Security Policy and security documentation;
- b) coordinating and monitoring the implementation of the security measure on the basis of information from monitoring and surveillance systems or decisions of the KB Committee;
- c) acquainting the KB Committee with the prepared plan for the development of security awareness;
- d) ensuring:
 - processing and regular updating of Asset and Risk Assessment Reports and the Declaration of Applicability;
 - regular risk assessment with suppliers, carrying out checks on security measures in place for the services provided and applying contractual conditions to ensure that identified cyber security deficiencies are addressed;

- updating the SŘBI and the relevant documentation, based on the results of audits or significant changes, and evaluating the effectiveness of security measures;
 - elaboration and updating of the risk management plan;
 - implementation of reactive measures issued by the NÚKIB;
 - synergies in carrying out audits carried out by the NÚKIB or the cyber security auditor;
- e) defining and controlling the process of dealing with a cyber security case or incident;
- f) setting rules for suppliers of ICT components, systems and services in contracts, which take the needs of the SŘBI into account and taking them into account for suppliers or other persons involved in the development, operation or security of information systems included in the scope of the SŘBI.
- g) regular submission of a report to the KB Committee with at least:
- evaluation of identified cyber risks;
 - detected cyber security incidents;
 - revealed cyber incidents;
 - proposals to mitigate unacceptable risks;
 - proposals to change the priorities of security projects.