BRNO UNIVERSITY OF TECHNOLOGY

Full text as of: 1. 4. 2025
Incorporates: Amendment 1

GUIDELINE NO 1/2024
CYBER AND INFORMATION SECURITY MANAGEMENT AT THE UNIVERSITY

Article 1
Course and purpose of the regulation

1. In accordance with the legal regulations governing cyber security, this Guideline defines the persons responsible for cyber and information security management (hereinafter referred to as cyber security) at the BUT and sets out their rights and obligations.
2. The purpose of this Guideline is to ensure cyber security and resilience according to standards arising from generally binding legislation, including the establishment of objective procedures for setting, implementing and evaluating specific measures.
3. The implementation of specific measures to ensure cyber security is the employment obligation of each employee. Managers are responsible for the implementation of specific measures and procedures in the workplaces they manage as part of their duties.

Article 2
Management organisation (roles)

1. Followin roles are established to manage cyber security at the BUT:
   a. Cybersecurity Manager (hereinafter referred to as "CS Manager"),
   b. Cybersecurity Architect (hereinafter referred to as "CS Architect"),
   c. Cybersecurity Auditor (hereinafter referred to as "CS Auditor").
2. The Asset Guarantors shall participate in cyber security management within the scope of their competencies as set out in the internal regulations and organisational documents, as set out in Article 6 of this Guideline.
3. A special guideline[1] establishes the Cybersecurity Committee (hereinafter referred to as the "CS Committee").
4. CS Manager and CS Architect are positions within the Centre of Information Services of the BUT (hereinafter referred to as "CIS").

[1] Guideline No. 5/2021 - Advisory Boards and Working Groups established in accordance with the Statute of BUT

5. The role of the CS Auditor is carried by an authorised employee of the Internal Audit and Control Department of the Rector´s Office of the BUT.

Article 3
Cyber Security Manager

1. The CS Manager shall communicate with the National Cyber and Information Security Agency (hereinafter referred to as the "NUKIB") in the context of ensuring cyber security, including the fulfilment of the reporting obligation in dealing with cyber security events and incidents

2. In particular, the CS Manager shall:
   a. record individual assets and provide information and assistance to Asset Guarantors,
   b. coordinate the handling of cyber security events and incidents
   c. coordinate activities to ensure the security of information assets,
   d. plan and manage cybersecurity projects approved by the CS Committee,
   e. issue the Rules for Ensuring Cyber and Information Security in accordance with Article 8a.
   f. administer the information security management system,
   g. perform risk analysis for assets of record,
   h. convene and prepare documents for the meetings of the CS Committee,
   i. participate in the preparation of the Cybersecurity Strategy of the BUT,
   j. notifiy the NUKIB of security incidents in accordance with applicable legislation,
   k. provide documents for the CS Auditor and the BUT authorities.

3. In carrying out activities under this Directive, the KB Manager is authorised to:
   a. request information and cooperation from the Asset Guarantors, including, where appropriate, the preparation of necessary documents for risk management or the implementation of specific measures
   b. request an audit from KB's Auditor,
   c. request a decision from the KB Committee on the acceptability or unacceptability of identified cyber security risks, including the determination of an acceptable level of risk and a financial limit for the elimination of unacceptable risks.

4. The CS Manager shall be appointed and removed by the Rector upon the proposal of the CIS Director.

Article 4
Cybersecurity Architect

1. The CS architect shall propose appropriate cybersecurity procedures and measures, their design and implementation procedure so that their implementation is achievable within the available technical and financial resources.

2. CS Architect in particular shall:
   a. keep all documentation produced by it pursuant to paragraph 1 up to date,
   b. identify risks and proposes measures to reduce them,
   c. prepare documents for the CS Manager and CS Auditor,
   d. contribute to the development of the cyber security strategy,
   e. propose preventive measures leading to the maintenance of the information security management system and cyber security in general at the BUT.

3. In performing activities under this Guideline, the CS Architect is entitled to:
   a. request information and assistance from the CS Manager in the preparation of documents,
   b. request documentation from the Asset Guarantors.

4. Within the scope of its activities, CS Architect prepares in particular:
   a. the definition of an information security management system,
   b. development analysis and risk evaluation methodology,
   c. model of the evaluation's cyber and information security architecture,
   d. process model for cybersecurity management,
   e. a plan for implementing security measures,
   f. definition of tests for verification of security measures.

   The CS architect is responsible for the effectiveness of the measures he/she proposes, but is not responsible for the implementation of the specific measures he/she proposes.

6. The CS Architect is appointed and dismissed by the Rector on the proposal of the CIS Director.

Article 5
Cybersecurity Auditor

1. The CS Auditor shall supervise the implementation of the models and measures proposed by the CS Architect, in particular by verifying the compliance of the implementation with the proposed solution and randomly checking the systems for undocumented deviations that would increase the risk of cyber threats.
2. In addition to the ongoing activities defined in the previous paragraph, CS Auditor:
   a. draw up a final report on the implementation of the measures,
   b. produce an interim report on the implementation of the cyber security strategy
   c. performs an audit at the request of the KB Manager and informs him of the result,
   d. conducts an audit of the asset, at the request of the Asset Guarantor, and informs it of the result,
   e. informs the CS Committee of the results of the audit.

3. Within the scope of its activities, the CS Auditor is authorised to:
   a. request documents from the CS Manager and Asset Guarantors,
   b. to inform the CS Committee of the result of the audit,
   c. request additional information from CS Architect.

4. The CS Auditor is appointed and dismissed by the Rector on the proposal of the Head of the Internal Audit and Control Department.

Article 6
Asset guarantor

1. In accordance with generally binding legal regulations[2] , an asset or information asset means any data, information, Transfer, software, hardware, services, or equipment that are of value to the BUT and whose confidentiality, integrity and availability, loss, theft or misuse would make it difficult for the BUT to operate or cause any harm.
2. The guarantor of an asset is the person responsible for a particular asset and who executes all Resolutions related to it.

[2] Act No. 181/2014 Coll. on Cyber Security

3. In particular, the guarantor of the asset is obliged to:
   a. granting authorities to persons referred to in Article 2(1) with the information for the evaluation of risks,
   b. apply the individual measures and obligations arising from the approved documents,
   c. cooperate with CS Manager and CS Auditor.

4. The asset sponsor may, in the performance of its duties in relation to cybersecurity:
   a. request an exemption from the CS Cybersecurity Policy from the CS Manager,
   b. request an extraordinary audit from CS Auditor.

Article 7
Cybersecurity Committee

1. The CS Committee is a permanent collective body, whose activities and composition are regulated by a specific guideline.

2. CS Committee in particular:
   a. Approves the BUT Cyber Security Strategy on the proposal of the CS Manager,
   b. approves the documents prepared by the CS Architect,
   c. evaluates the state of cybersecurity of the BUT.

Article 8
Cyber security events and incidents

1. In the event that a cyber security event ("Event") or cyber security incident ("Incident") is detected, each employee is required to take the necessary steps to eliminate any potential harm.

2. The manager of the workplaces where the Event or Incident occurred is obliged to immediately inform the CS Manager about the Event or Incident.

3. In the event of an Incident, the CS Manager shall ensure that the NUKIB and, within a reasonable time, the CS Committee are informed within the statutory time limits.

4. In the event that a Serious Incident is detected, the CS Manager shall always request the Auditor to conduct an audit in accordance with the procedure set out in Article 5(2)(c). In the event of an Incident, the same procedure shall be followed if the CS Committee so decides.

Article 8a
Cyber and information security assurance

1. The CS Manager in accordance with his/her activities pursuant to Article 3 of this Guideline, shall issue binding Rules for ensuring cyber and information security (hereinafter referred to as the "KB Rules") after approval by the KB Committee, so that these Rules together form the basic framework of the obligations of all persons using the cyberspace of the BUT.

2. The CS Rules pursuant to the preceding paragraph include, in particular, the setting up of the Information Security Management System (hereinafter referred to as "ISMS"), the procedures

and rules following from the specific ISMS settings, and the legal requirements for ISMS as defined by generally binding legal regulations.

3. The CS Manager shall ensure that the CS Rules are published on the website https://vut.cz/kybez and shall inform the Deans, Directors of University Institutes and Directors of other units through the Rector. Every user of the cyberspace of the BUT is then obliged to familiarize himself with the CS Rules published in this way.

4. All asset owners are obliged to carry out regular assessments within the assets under their management.

5. Deans, directors of university institutes and directors of other units are obliged, for the purpose of proper setup, to identify the persons responsible for the implementation of the activities defined in the CS Rules and to communicate this information to the CS manager.

6. CS Manager shall:
   a. maintain a list of the persons defined in paragraph 5,
   b. evaluate and update, if necessary, the wording of the CS Rules.
   c. evaluate compliance with the CS Rules and reports any non-compliance to the CS Committee.

Article 9
Final provisions

1. The Rector shall appoint the CS Manager, the CS Architect, the CS Auditor and the members of the CS Committee within 30 days of the entry into force of this Guideline.

2. This Guidline shall enter into force on the date specified in its heading.

associate professor. Ing. Ladislav Janíček, Ph.D., MBA, LL.M.
Rector