University of South Bohemia in České Budějovice

Document designation:	**ISMS-000**
Document title:	**Basic Information Security Policy**
TLP category:	TLP:CLEAR
Scope:	The policy is intended for all USB employees, students, and participants in lifelong learning, suppliers, and organisations collaborating with USB or other interested parties.
Legislation element:	Act No 181/2014, on Cyber Security Decree No 82/2018, on Cyber Security
Release Date:	6. 12. 2024
Effective date:	**6. 12. 2024**
Validity until:	until further notice
Number of pages + annexes:	2 + 0
Version:	1.0
The importance and benefits:	The importance of the policy is to define the main principles, objectives, security needs and rights and obligations in relation to information security management at the University of South Bohemia in České Budějovice for all stakeholders.
Storing:	Public part of the USB wiki website
It revokes documents:	
Prepared by:	Jan Urbánek – Manager CS USB
Reviewed by:	Cyber Security Management Committee USB
Approved by:	Rector USB

Information announcement

This policy is issued on the basis of Act No 181/2014, on Cyber Security and on Amendments to Related Acts (Cyber Security Act), as amended, and its implementing regulations, in particular, Decree No 82/2018, on Security Measures, Cyber Security Incidents, Reactive Measures, Submission Requirements in the Area of Cyber Security and Data Disposal (Cyber Security Decree).

This policy is part of the security policy in the area of the information security management system within the University of South Bohemia in České Budějovice (hereinafter referred to as '*USB*').

The security policy also builds on the Rector's Ordinance R 511[1] in the context of ensuring the cyber security of USB.

(a) Main principles, objectives and security needs

USB recognises the existence of real cyber security threats and the importance of ensuring cyber security at USB ('*CS USB*') for the seamless fulfilment of USB's mission and activities.

USB recognises its responsibility for CS USB and therefore commits to actively support the adequate provision of CS USB in accordance with USB strategy.

USB will also actively participate in evaluating the effectiveness of the Information Security Management System (*ISMS*), ensuring the CS USB, and providing the appropriate resources necessary to achieve the CS USB objectives.

In order to achieve the above, USB commits to:

- establish and implement an ISMS, together with defining the scope and boundaries of the overall system,
- operate, monitor, review, maintain and continuously improve the ISMS (PDCA cycle),
- ensure the definition of ISMS objectives and a plan for achieving them,
- identify roles, rights and responsibilities in the ISMS area,
- carry out internal audits of the ISMS,
- provide resources for all stages of the life cycle of the ISMS.

The term **information security** is understood as the process of ensuring that information is protected at the necessary level to ensure its integrity, availability and confidentiality on an ongoing basis.

The main objectives of USB in the area of CS are to ensure that:

- USB information assets are adequately protected in terms of the above information security term,

[1] Rector's Ordinance R 511, on ensuring cyber security at USB

- the security risks of information assets associated with the operation of USB are effectively managed,
- processes are set up and controlled to ensure CS,
- the security measures are in accordance with the applicable cyber security legislation of the Czech Republic or are based on internationally recognised standards and recommendations.

Individual security objectives are met by implementing adequate personnel, organisational, procedural or technical measures determined within the risk management process and in accordance with legislative requirements and relevant standards or norms.

(b) Rights and obligations in relation to information security management

All descriptions of the rights and obligations of individual roles in relation to information security management are regulated by the Rector's Ordinance R 511.[1]

(c) Scope and limits of the ISMS USB

The USB ISMS applies to all USB units and constituent parts, all USB employees, students and USB lifelong learning participants. Further, the scope of the ISMS within USB includes all information, assets, supporting assets, processes, and other procedures involved in the operation of significant USB information systems. The scope of the ISMS also includes services and products provided by external vendors that are involved in the operation of USB major information systems.

ISMS USB covers all 23 security policy areas according to the Cyber Security Decree.

d) Preparation of documentation CS and ISMS USB

Individual policies, guidelines, procedures and processes, methodological manuals and other information associated with the CS USB and ISMS are internal only and will only be available to USB employees or students and LLL participants. All internal CS USB and ISMS documents are only accessible by logging into the USB Wiki website – https://wiki.jcu.cz/.

The relevant exception is this Basic Information Security Policy, including all annexes and other related documents that are specifically mentioned.

Revision history

Version 1.0 – Document creation