University of South Bohemia in České Budějovice

Document identification:	**ISMS-S-001**
Document title:	**Remote work**
Document type:	Internal directive of USB
Scope:	This directive applies to all employees of USB who request remote work and use technical equipment owned by USB to perform their work activities.
Legislative element:	Rector's measure R 602
Date of issue:	04. 09. 2025
Effective date:	**04. 09. 2025**
Valid until:	Until revoked
No. pages + attachments:	4 + 0
Version:	1.2
Purpose and benefits:	The purpose of the directive is to ensure data security during remote work and to define requirements for secure access to the USB network from an external workplace.
Storage:	ISMS section on the USB wiki – wiki.jcu.cz
Superseded documents:	ISMS-010_Homeworking + attachements
Prepared by:	Jan Urbánek - Cybersecurity manager USB
Reviewed by:	USB Cybersecurity committee
Approved by:	USB Cybersecurity committee

Information notice

Before starting remote work, this form of activity must be demonstrably approved for USB employees. To comply with the approval procedure, it is necessary to respect the Rector's Measure for the performance of work by employees of the University of South Bohemia in České Budějovice (USB) outside the employer's workplace – remote work R602 dated 03. 9. 2023

a) Request and its approval

The employee must justify the need for remote work in a written request, and if confirmed by their supervisor, it must be approved by the department head. Before starting remote work, the form *ISMS-S-001_Remote_Work_Permission* (Annex 1 of the Rector's measure R 602), confirmed by the relevant staff of the USB unit (rector/dean, section/unit head, supervisor, OHS technician), must be completed and submitted to the HR department.

b) Connection to the JU network

USB does not provide connectivity setup for employees/users working remotely. First, the external workplace must be connected to the internet and then access to the USB network must be established via a VPN concentrator. This is an encrypted connection to the internal USB network via the internet under a USB IP address.

1. **Access to the USB network**

To access selected USB servers or university information systems (IS) such as FIS, MIS, STAG, EGJE, etc., the following conditions must be met:

I. The user's computer must have an active internet connection and a VPN concentrator installed as chosen by the USB VPN administrator[1];

II. The user must have a university account and a configured freeradius password. To do this, they must log in with their university credentials to the IDM service (https://idm.jcu.cz) and select "Change freeradius password";

c) IT Security Rules

1. **What the remote user must comply with:**

- Access to USB information systems must always be via encrypted VPN connection;
- After approval of the remote work request, the user must first discuss access options and connection parameters to pre-approved USB ICT services with their unit's IT manager, who may cooperate with system administrators as needed;

[1] A detailed description and instructions for this process can be found at: https://wiki.jcu.cz/VPN.

- If the user needs expert help while accessing university-wide information systems remotely, they should contact the USB HelpDesk at: https://servicedesk.jcu.cz;
- The company computer used for remote work must be checked by the unit's IT administrator and equipped with necessary software to protect against unauthorized internet access and malicious code or other security threats;
- Access to the company computer must be secured with a user account and password, and these credentials must be protected against misuse;
- The remote user must back up their work results and promptly store backups either on external media, the user's university M365 cloud storage, or a designated server in the USB network (as agreed with the unit's IT administrator);
- If the user has a private email address recorded in IDM that does not have the jcu.cz domain, it must be kept up-to-date and fully functional to enable mutual communication between the user and USB.

2. **The remote user must not:**

- Perform illegal activities on USB-owned computers, such as downloading unauthorized content (music, videos, etc.) from the internet;
- Use USB computers for personal commercial purposes (providing information, programs, or data for payment);
- Allow other persons (e.g., family members) to access entrusted ICT resources (computer, printer, accessories);
- Leave the computer used for remote work (if portable) in a car or elsewhere outside the external workplace without increased supervision;
- Log into USB IS without VPN and via unsecured wireless networks:
  - Typically FreeWiFi at airports, hotels, restaurants, and other locations;
- Log into USB IS via unsecured wireless networks:
  - Networks with only WEP or WPA encryption;

The user must also follow USB ISMS security policies and associated directives available at https://wiki.jcu.cz/.

d) Software and Hardware

1. **Software**

The user may only use legal software with a USB-assigned license or freeware and must comply with the defined license terms.

The computer system must promptly install update packages (automatic updates) issued by the operating system manufacturer and other installed software applications.

2. Hardware

The remote user is not authorized to modify the hardware configuration or BIOS of the USB-provided computer without prior approval from their supervisor and unit IT administrator.

3. Repairs and servicing of entrusted equipment

Software and hardware issues must be reported to the unit's IT administrator. If the issue cannot be resolved remotely, the employee may be asked to deliver the computer to a designated location as agreed.

e) Information Protection

The remote user must not disseminate protected USB information (all information and data that must be protected from unauthorized access) or allow its misuse by third parties. This includes business contracts, know-how, operational methods, procedures, workflows, concepts, strategies, and personal data under Act No. 110/2019 Coll. and subsequent regulations. The user must comply with copyright law and all legal regulations related to information protection.

If an employee accesses sensitive personal data of students, employees, partners, and companies cooperating with JU, in accordance with the above-mentioned law, or other sensitive data of JU, and transfers and stores this data on their PC, it is necessary to encrypt it.

ICT resources entrusted for remote work must be protected against damage and misuse and handled according to the manufacturer's instructions and the unit IT administrator's guidance or regulations.

f) Occupational Health and Safety (OHS) and Fire Protection

USB employees working remotely must follow the same rules and instructions regarding occupational health and safety and fire protection as if working on-site at USB. They were instructed by the USB OHS and Fire Protection technician and confirmed this by signing their employment contract with USB. Any changes in related laws will be communicated to the employee via email.

Remote work may only begin after the mentioned instruction and confirmation of Annex No. 1 of the Rector's measure R 602, along with approval by other required staff.

In case of inspection of OHS and Fire Protection compliance by USB, the remote worker must allow the USB OHS and Fire Protection officer to enter their home environment under pre-agreed conditions.