COLLECTION OF DECISIONS AND ORDINANCES OF UNIVERSITY OF SOUTH BOHEMIA IN ČESKÉ BUDĚJOVICE

Number: R 626 Date: 10 February 2026

Rector's Ordinance establishing rules for working with user data at the University of South Bohemia in České Budějovice

Article 1
Introductory provisions

1. This ordinance regulates the rules for storing, processing, sharing, backing up, deleting and other handling of user data of employees and students of the University of South Bohemia in České Budějovice (hereinafter referred to as '**USB**').

2. The operator of data storage and management services is the Centre of Information Technology (hereinafter referred to as 'CIT') and the IT offices of the constituent parts of USB.

3. Central data storage services are provided in the USB local infrastructure environment (server storage of constituent parts) and in the Microsoft 365 cloud (OneDrive for Business / SharePoint) within the available capacities. It is also possible to use local encrypted storage (local drives in workstations or mobile devices, external drives, NAS storage, etc.) owned by USB. The storage is intended for users to carry out their work and study obligations. The storage is not intended for storing users' private data.

4. Users are required to use only their USB user account and storage in accordance with Article 1, paragraph 3 to fulfil their work obligations.

5. Storage capacities may be limited by quotas. Once the quota is reached, storage may be blocked. Users are required to prevent capacity overuse, to use storage space efficiently, and, if necessary, to request assistance in a timely manner with capacity increases or maintenance of the allocated storage space.

6. In order to protect USB property, IT security and data, operations (storage, sharing and other handling of data) are monitored and recorded in the scope of operational and security data (telemetry, access audit). The content of files may only be accessed in the context of resolving security incidents or in other justified cases (Article 7(4)), in compliance with personal data protection rules.

Article 2
Terms and scope

1. **User data** refers particularly to files and documents created in the course of work and study duties and other files, in particular technical and operational files necessary for the operation of USB remits.

2. **The data owner (user)** refers to an employee or person in another similar relationship with USB, a student, and other persons who have a USB user account and who create user data in the course of their activities or store it in their user account or in one of the storage facilities.

3. **A workstation** is defined as a device owned by USB or the user and used to work with USB services.

4. **Server storage** is central storage managed by CIT or the IT departments of individual faculties and other constituent parts of USB (profile storage, personal drive H:/ (HOME), network shared folders, etc.).

5. **OneDrive for Business** is personal work cloud storage within Microsoft 365 assigned to a specific user.

6. **Microsoft Teams/Sharepoint** is group cloud storage within Microsoft 365 assigned to a group of users, which is managed centrally or by selected users.

7. **External storage** refers to various types of storage provided by third parties, such as CESNET storage (OwnCloud, data storage, MetaCentrum, etc.) or storage used within projects at USB.

Article 3
Classification and placement of data

1. Data is divided into categories according to the ISMS USB cyber security directive: public / internal / confidential. Users are required to protect data appropriately.

2. Internal and confidential data shall be stored primarily on USB server storage or OneDrive; storage on local and external drives is only possible if the device is encrypted (e.g. using BitLocker).

3. It is prohibited to store sensitive, internal and confidential data through unauthorised services and on unencrypted portable media. Sensitive data is, in particular, data that contains personal information.

Article 4
Access, sharing and delegation

1. The data owner (user) may share data with other USB users to a reasonable extent. The data owner (user) is responsible for the accuracy and appropriateness of such sharing, or for setting the appropriate permissions for accessing the data. Data sharing is appropriate if other users need access to the shared data in order to perform their work or study duties, or to ensure the substitutability of employees or the transfer of work remits between employees.

2. External data sharing outside USB is only permitted on the basis of a name (to specific identities), with a limited link validity period and to the extent necessary for the purpose of sharing. Data containing personal information may be shared with third parties outside USB in compliance with personal data protection rules.

3. Automated transfer of any data to unauthorised storage locations is prohibited.

4. The CIT or the relevant IT office of the constituent part may set up access for another user, on the basis of a justified written consent of the data owner (a consent form template is attached to this ordinance) or a justified decision of the relevant manager referred to in Articles IV and V of USB Rector's Ordinance No. R 378, which establishes rules for the protection and processing of personal data, after prior consultation with the data protection officer. All such accesses shall be recorded.

5. It is prohibited to transfer sensitive, internal and confidential data for processing to unsupported artificial intelligence (AI) applications and services, as well as to grant such applications or services access to this data. CIT is not obliged to allow connections to unverified and unsupported applications. A list of supported applications and services is available at **wiki.jcu.cz**. Details on the use of artificial intelligence are governed by a separate ISMS cyber security policy.

Article 5
Security of end devices (workstations, laptops, mobile devices)

1. Devices owned by USB are managed by CIT or the IT office of the relevant unit.

2. Devices must have drive encryption, an up-to-date operating system, an active automatic screen lock, an active firewall, and anti-malware.

Article 6
Backup, version control, and recovery

1. Server storage managed by CIT USB is backed up according to the plan available at **wiki.jcu.cz**.

2. OneDrive and SharePoint (including team storage) use version control, and authorised users can manage and restore previous versions of data themselves.

3. Employees' OneDrive is backed up. Recovery requests are handled by CIT. The data owner or competent person must submit a written request for recovery via ServiceDesk.

4. It is possible to request backup of teams in MS Teams and SharePoint. Restoration requests are handled by CIT. The data owner or competent person must submit a written request for restoration via ServiceDesk.

5. The data owner (user) is fully responsible for backing up data stored on local drives in workstations or mobile devices, on external drives, in NAS storage, etc. CIT and the IT offices of the constituent parts of USB are not responsible for backing up this data.

Article 7
Retention and deletion

1. Data is stored for the duration of the user's valid employment or other similar relationship with USB and in accordance with applicable legal and internal regulations.

2. After the termination of the employment or other similar relationship, the OneDrive personal storage remains active for 90 days, but the user no longer has access to it. After this period, the data is deleted.

3. After graduation, the personal OneDrive storage remains active and accessible for 180 days (waiting period). After that, the storage is made inaccessible and the data is deleted.

4. In the event of a user's long-term absence and the existence of a legitimate interest, the employer may obtain access exclusively to work data by decision of the authorised managers specified in Articles IV and V of Rector's Ordinance R 378, which establishes rules for the protection and processing of personal data, after prior consultation with the Data Protection Officer. All such accesses are recorded.

5. USB does not export data from any storage at the request of users if their employment or other similar relationship with USB has been terminated or the user has completed their studies. Exceptions are decided on by the authorised managers listed in Articles IV and V of Rector's Ordinance R No. R 378, which establishes rules for the protection and processing of personal data, after prior consultation with the Data Protection Officer.

Article 8
Shared storage

1. Shared storage (e.g. team SharePoints, network shared drives) is not linked to specific individuals. Its creation and access management are carried out by CIT or the staff of IT offices at the constituent units.

2. Data owners (users) are advised to regularly review the membership of other users in shared storage groups (e.g. in team storage on SharePoint) and to check the access permissions that have been set.

Article 9
Audit, incidents and responsibility

1. CIT or IT offices of constituent parts of USB perform regular audits of access and sharing; violations of the rules are dealt with in accordance with USB labour and study regulations.

2. Security incidents are reported to the USB Service Desk. CIT keeps records and ensures that corrective measures are taken.

Article 10
Final provision

This ordinance comes into force and takes effect on the date of its announcement and publication in the public section of the USB website.

prof. Ing. Pavel Kozák, Ph.D.
Rector

Prepared by: USB Centre of Information Technology, Cyber Security Manager
Distribution list: USB management, faculty deans, directors of all constituent parts of USB

Annexe: Consent to disclose user data to another user