SBÍRKA ROZHODNUTÍ A OPATŘENÍ
JIHOČESKÉ UNIVERZITY V ČESKÝCH BUDĚJOVICÍCH

číslo: R 626 datum: 10. 2. 2026

Opatření rektora,
kterým se stanoví pravidla
pro práci s uživatelskými daty na Jihočeské univerzitě v Českých Budějovicích

Článek 1
Úvodní ustanovení

1. Toto opatření upravuje pravidla pro ukládání, zpracování, sdílení, zálohování, mazání a další nakládání s uživatelskými daty zaměstnanců a studentů Jihočeské univerzity v Českých Budějovicích (dále jen „**JU**“).

2. Provozovatelem služeb ukládání a správy dat je Centrum informačních technologií JU (dále jen „**CIT**“) a IT pracoviště jednotlivých součástí JU.

3. Centrální služby ukládání dat jsou poskytovány v prostředí lokální infrastruktury JU (serverová úložiště součástí) a v cloudu Microsoft 365 (OneDrive for Business / SharePoint) v rámci dostupných kapacit. Dále je možné využívat lokální šifrovaná úložiště (lokální disky v pracovních stanicích či mobilních zařízeních, externí disky, NAS úložiště atp.), která jsou v majetku JU. Uložiště jsou určena k plnění pracovních a studijních povinností uživatelů. Uložiště nejsou určena pro ukládání soukromých dat uživatelů.

4. Uživatelé jsou povinni používat k plnění pracovních povinností výhradně svůj uživatelský účet JU a úložiště dle článku 1 odstavce 3.

5. Kapacity úložišť mohou být omezeny kvótou. Při naplnění kvóty může být zablokováno ukládání. Uživatelé jsou povinni přeplnění kapacit předcházet a využívat úložný prostor hospodárně a v případě nutnosti včas požádat o pomoc s navýšením kapacit nebo údržbou přiděleného prostoru.

6. Za účelem ochrany majetku JU, bezpečnosti IT a dat je provoz (ukládání, sdílení a další nakládání s daty) monitorován a zaznamenáván v rozsahu provozních a bezpečnostních údajů (telemetrie, audit přístupů). Obsah souborů může být zpřístupněn pouze v rámci řešení bezpečnostních incidentů nebo v dalších odůvodněných případech (článek 7 odst. 4) za dodržení pravidel pro ochranu osobních údajů.

Článek 2
Pojmy a rozsah

1. **Uživatelskými daty** se rozumí zejména soubory a dokumenty vzniklé při plnění pracovních a studijních povinností a další, zejména technické a provozní soubory nezbytné pro chod agend JU.

2. **Vlastníkem dat (uživatelem)** se rozumí zaměstnanec nebo osoba v jiném obdobném vztahu k JU, student a další osoby, které mají zřízený uživatelský účet JU a při své činnosti vytvoří uživatelská data nebo je mají uložená v rámci svého uživatelského účtu nebo na některém z úložišť.

3. **Pracovní stanicí** se rozumí zařízení v majetku JU nebo uživatele používané k práci se službami JU.

4. **Serverové úložiště** je centrální úložiště spravované CIT nebo IT pracovišti jednotlivých fakult a ostatních součástí JU (profilová úložiště, osobní disk H:/ (HOME), síťové sdílené složky atp.).

5. **OneDrive for Business** je osobní pracovní cloudové úložiště v rámci Microsoft 365 přidělené konkrétnímu uživateli.

6. **Microsoft Teams/Sharepoint** je skupinové cloudové úložiště v rámci Microsoft 365 přidělené skupině uživatelů, které je spravováno centrálně nebo vybranými uživateli.

7. **Externími úložišti** jsou různé druhy úložišť poskytované třetími stranami, například úložiště sdružení CESNET (OwnCloud, datová úložiště, MetaCentrum, atp.) či úložiště používaná v rámci řešených projektů na JU.

Článek 3
Klasifikace a umísťování dat

1. Data se dělí dle směrnice kybernetické bezpečnosti ISMS JU na kategorie: veřejná / interní / důvěrná. Uživatelé jsou povinni data odpovídajícím způsobem chránit.

2. Interní a důvěrná data se ukládají přednostně na serverová úložiště JU nebo OneDrive, ukládání na lokální a externí disky je možné jen za podmínky šifrování zařízení (např. pomocí nástroje BitLocker).

3. Je zakázáno ukládat citlivá, interní a důvěrná data na neschválené služby a nešifrovaná přenosná média. Citlivá data jsou zejména taková, která obsahují osobní údaje.

Článek 4
Přístup, sdílení a delegace

1. Vlastník dat (uživatel) může v přiměřené míře sdílet data s dalšími uživateli JU. Za správnost a přiměřenost takového sdílení, resp. nastavení příslušného oprávnění k přístupu k datům nese odpovědnost jejich vlastník (uživatel). Sdílení dat je přiměřené, pokud ke sdíleným datům mají mít přístup další uživatelé z důvodu toho, že je potřebují k plnění svých pracovních nebo studijních povinností nebo z důvodu zajištění zastupitelnosti zaměstnanců nebo předání pracovní agendy mezi zaměstnanci.

2. Externí sdílení dat mimo JU je povoleno pouze jmenovitě (na konkrétní identity), s omezenou dobou platnosti odkazu a v rozsahu nezbytném pro účel sdílení. Data obsahující osobní údaje mohou být s třetími osobami mimo JU sdílená za dodržení pravidel ochrany osobních údajů.

3. Automatizované předávání jakýchkoliv dat do neschválených úložišť je zakázáno.

4. CIT nebo příslušné IT pracoviště součásti může na základě odůvodněného písemného souhlasu vlastníka dat (vzor souhlasu je přílohou tohoto opatření) nebo z odůvodněného rozhodnutí příslušného vedoucího pracovníka uvedeného v článcích IV a V opatření rektora č. R 378, kterým se stanoví pravidla pro ochranu a zpracování osobních údajů, a to po předchozí konzultaci s pověřencem pro ochranu osobních údajů, nastavit přístup jinému uživateli. Veškeré takové přístupy se evidují.

5. Je zakázáno předávat citlivá, interní a důvěrná data ke zpracování nepodporovaným aplikacím a službám umělé inteligence (AI), jakožto i udělit takovým aplikacím nebo službám k těmto datům přístup. CIT není povinen povolit připojení neověřeným a nepodporovaným aplikacím. Seznam podporovaných aplikací a služeb je dostupný na **wiki.jcu.cz**. Podrobnosti o využívání umělé inteligence upravuje samostatná směrnice kybernetické bezpečnosti ISMS.

Článek 5
Bezpečnost koncových zařízení (pracovní stanice, notebooky, mobilní zařízení)

1. Zařízení v majetku JU spravuje CIT nebo IT pracoviště součásti.

2. Zařízení musí mít šifrování disku, aktuální operační systém, aktivní automatický zámek obrazovky, aktivní firewall a antimalware.

Článek 6
Zálohování, verzování a obnova

1. Serverová úložiště spravovaná CIT JU jsou zálohována dle plánu dostupného na **wiki.jcu.cz**.

2. OneDrive, SharePoint (včetně týmových úložišť) využívají verzování a oprávnění uživatelé si mohou sami spravovat a obnovovat předchozí verze dat.

3. OneDrive zaměstnanců je zálohován. Požadavky na obnovu řeší CIT. Žádost o obnovu musí vlastník dat nebo kompetentní osoba podat písemně přes ServiceDesk.

4. Je možné požádat o zálohování týmů v MS Teams a Sharepoint. Požadavky na obnovu řeší CIT. Žádost o obnovu musí vlastník dat nebo kompetentní osoba podat písemně přes ServiceDesk.

5. Za zálohování dat uložených na lokálních discích v pracovních stanicích či mobilních zařízeních, na externích discích, v NAS úložištích atp. je plně zodpovědný vlastník dat (uživatel). CIT a IT pracoviště jednotlivých součástí JU nenesou za zálohování těchto dat odpovědnost.

Článek 7
Retence a mazání

1. Data jsou uchovávána po dobu platného pracovněprávního nebo jiného obdobného vztahu uživatele k JU a v souladu s platnými právními a interními předpisy.

2. Po ukončení pracovněprávního nebo jiného obdobného vztahu zůstává osobní úložiště OneDrive aktivní 90 dní, ale uživatel do něj již nemá přístup. Po uplynutí této doby jsou data smazána.

3. Po ukončení studia zůstává osobní úložiště OneDrive aktivní a přístupné 180 dní (karenční doba). Poté je úložiště znepřístupněno a data jsou smazána.

4. Zaměstnavatel může při dlouhodobé nepřítomnosti uživatele a existenci oprávněného zájmu získat přístup výhradně k pracovním datům, a to rozhodnutím oprávněných vedoucích uvedených v článcích IV a V opatření rektora č. R 378, kterým se stanoví pravidla pro ochranu a zpracování osobních údajů, a to po předchozí konzultaci s Pověřencem pro ochranu osobních údajů. Veškeré takové přístupy se evidují.

5. JU neprovádí export dat na žádost uživatelů z žádného úložiště, pokud došlo k ukončení jejich pracovněprávního nebo jiného obdobného vztahu k JU nebo k ukončení studia uživatele. O výjimkách rozhodují oprávnění vedoucí uvedení v článcích IV a V opatření rektora č. R 378, kterým se stanoví pravidla pro ochranu a zpracování osobních údajů, a to po předchozí konzultaci s Pověřencem pro ochranu osobních údajů.

Článek 8
Sdílená úložiště

1. Sdílená úložiště (např. týmové SharePointy, síťové sdílené disky) nejsou vázány na konkrétní osoby. Jejich zřizování a správa přístupů probíhá prostřednictvím CIT nebo zaměstnanců IT pracovišť součástí.

2. Vlastníkům dat (uživatelům) se doporučuje provádět pravidelné revize členství ostatních uživatelů ve skupinách sdílených úložišť (např. v týmových úložištích na SharePointu) a kontrolovat nastavená přístupová oprávnění.

Článek 9
Audit, incidenty a odpovědnost

1. CIT nebo IT pracoviště součástí provádí pravidelné audity přístupů a sdílení, porušení pravidel se řeší dle pracovněprávních a studijních předpisů JU.

2. Bezpečnostní incidenty se hlásí na Service Desk JU. CIT vede evidenci a zajišťuje nápravná opatření.

Článek 10
Závěrečné ustanovení

Toto opatření nabývá platnosti a účinnosti dnem vyhlášení a zveřejnění ve veřejné části webových stránek JU.

prof. Ing. Pavel Kozák, Ph.D.
rektor

Zpracoval: Centrum informačních technologií JU, manažer kybernetické bezpečnosti
Rozdělovník: vedení JU, děkani fakult, ředitelé všech součástí JU

Příloha: Souhlas se zpřístupněním uživatelských dat jinému uživateli