SBÍRKA ROZHODNUTÍ A OPATŘENÍ ŘEDITELE CIT
JIHOČESKÉ UNIVERZITY V ČESKÝCH BUDĚJOVICÍCH

číslo: **CIT_04** datum: **3. 11. 2026**

Opatření ředitele CIT, kterým se stanoví pravidla pro ukládání a sdílení hesel a dalších citlivých a důvěrných údajů

Článek 1
Úvodní ustanovení a účel opatření

1. Toto opatření stanoví pravidla, podle kterých zaměstnanci Centra informačních technologií Jihočeské univerzity v Českých Budějovicích (dále jen „CIT“ a „JU“) ukládají, spravují a sdílejí hesla, klíče, tokeny a další citlivé a důvěrné údaje, které slouží k přístupu ke službám, systémům a aktivům ve správě CIT.
2. Cílem opatření je zajistit, aby tyto údaje byly uloženy na jednom zabezpečeném místě, byly dostupné oprávněným osobám i v době nepřítomnosti jednotlivce nebo při obnově po havárii, nebyly předávány nezabezpečenými kanály a aby bylo možné prokázat řízení přístupu k nim.
3. CIT při plnění povinností podle tohoto opatření vychází zejména z těchto právních předpisů a vnitřních norem JU (vždy v jejich aktuálně účinném znění):
    - zákon č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“), v rozsahu povinností poskytovatele regulované služby v režimu vyšších povinností;
    - vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností;
    - zákon č. 110/2019 Sb., o zpracování osobních údajů;
    - zákon č. 262/2006 Sb., zákoník práce, zejména § 301 (povinnosti zaměstnanců);
    - nařízení (EU) 2016/679, obecné nařízení o ochraně osobních údajů (dále jen „GDPR“);
    - Statut Jihočeské univerzity v Českých Budějovicích;
    - opatření rektora č. R 634, kterým se vydává Organizační řád Rektorátu JU (vymezení působnosti CIT a jeho ředitele);
    - ostatní opatření ředitele CIT.
4. Toto opatření nenahrazuje návody a technické postupy; upravuje výhradně zacházení s citlivými a důvěrnými údaji.

Článek 2
Základní pojmy

1. **„Citlivým a důvěrným údajem“** se pro účely tohoto opatření rozumí zejména:
   - hesla a přihlašovací údaje uživatelských, administrátorských, servisních a technických účtů;
   - privátní klíče (SSH, TLS/SSL, PGP) a hesla k nim, soubory certifikátů s privátním klíčem (např. PFX/P12);
   - API klíče, přístupové tokeny, klientská tajemství (client secret) a sdílená tajemství (např. RADIUS, VPN PSK);
   - šifrovací hesla a klíče záloh a šifrovaných disků;
   - záchranné (recovery) kódy a tajemství vícefaktorového ověření technických a sdílených účtů;
   - přístupové údaje k administraci služeb externích poskytovatelů (např. CESNET, Microsoft 365);
   - licenční klíče a obdobné údaje, jejichž zneužití může JU způsobit škodu.
2. **„Vaultwardenem“** se rozumí správce hesel kompatibilní s aplikacemi Bitwarden, provozovaný CIT na infrastruktuře JU. Obsah trezorů je šifrován přímo v zařízení uživatele; server ani jeho správce obsah trezorů nevidí.
3. **„Organizacemi“** se rozumí sdílené prostory ve Vaultwardenu určené pro pracovní údaje jednotlivých útvarů CIT, členěné do **„sbírek“**, ke kterým se přiděluje přístup.
4. „**Osobní organizací“** se rozumí organizace v administrátorské instanci, kterou si zakládá konkrétní zaměstnanec, je jejím jediným členem a slouží výhradně k ukládání jeho jmenovitých účtů. Osobní organizace není organizací podle odst. 3.
5. **„Osobním trezorem“** se rozumí soukromá část účtu, ke které má přístup výhradně její držitel.
6. **„Odpovědným správcem“** se rozumí zaměstnanec CIT, který spravuje systém nebo oblast, k níž se sbírka vztahuje.
7. Pojmem **„Send“** se rozumí funkce Vaultwardenu pro jednorázové zabezpečené předání textu nebo souboru odkazem s omezenou dobou platnosti a počtem zobrazení.

Článek 3
Rozsah a závaznost

1. Toto opatření je závazné pro všechny zaměstnance CIT bez ohledu na formu pracovněprávního vztahu, včetně osob pracujících na dohodu.
2. Opatření se vztahuje na všechny IT služby, informační systémy, servery, síťové prvky, aplikace, cloudové služby a další technická aktiva, která CIT spravuje nebo za která odpovídá.
3. Citlivé a důvěrné údaje ke službám, systémům a aktivům ve správě CIT se ukládají a sdílejí výhradně prostřednictvím instancí Vaultwardenu. Mimo Vaultwarden se tyto údaje nezapisují, neposílají ani neuchovávají.
4. Přístupové údaje se ukládají podle toho, komu jsou přiděleny:
   - údaje, které nejsou přiděleny konkrétní osobě (technické, servisní a sdílené účty, klíče, certifikáty, tokeny, šifrovací hesla záloh apod.), se ukládají do organizací CIT v administrátorské instanci a musí být dostupné nejméně dvěma oprávněným osobám (odpovědný správce a jeho zástupce);

- jmenovité účty přidělené konkrétnímu zaměstnanci se ukládají do jeho osobní organizace v administrátorské instanci a nesdílejí se. Zastupitelnost se zajišťuje jmenovitým účtem zástupce, případně nejmenovitým účtem uloženým v organizaci útvaru.

5. Citlivé a důvěrné údaje se nesmějí předávat ani ukládat zejména prostřednictvím:
   - e-mailu, Microsoft Teams nebo jiného chatu, SMS a obdobných kanálů;
   - tiketů ServiceDesku, wiki JU, dokumentace aktiv;
   - souborů na SharePointu, OneDrive, sdílených discích nebo v lokálních souborech;
   - správců hesel integrovaných v prohlížeči a dalších neschválených správců hesel;
   - nástrojů umělé inteligence a online nástrojů (např. na generování či posouzení síly hesla);
   - papírových záznamů, s výjimkou záložních sad uložených v trezorech CIT.
6. Dokumentace aktiv a tikety obsahují místo samotného údaje pouze odkaz na jeho umístění ve Vaultwardenu (název sbírky a položky).

Článek 4
Údaje, které se do správce hesel neukládají

1. Ve Vaultwardenu se neukládají:
   - kódy k trezorům CIT a údaje, které jsou uchovávány výhradně fyzicky;
   - hlavní heslo k Vaultwardenu a záchranné kódy k vlastnímu vícefaktorovému ověření do Vaultwardenu;
   - hromadná data – exporty databází, seznamy osobních údajů třetích osob, dokumenty a zálohy; Vaultwarden slouží k ochraně přístupů k datům, nikoli k ukládání dat samotných.
2. Hlavní heslo a záchranné kódy k Vaultwardenu uchovává každý uživatel offline na bezpečném místě.

Článek 5
Instance správce hesel Vaultwarden

1. CIT provozuje tyto instance Vaultwardenu:

Instance	Určení
https://vw.jcu.cz	administrátorská instance – organizace útvarů CIT a osobní organizace zaměstnanců CIT, přístupná pouze přes administrátorskou VPN
https://pass.jcu.cz	uživatelská instance pro osobní trezory a pro předávání údajů dodavatelům (funkce Send)

2. Administrátorské a technické přístupové údaje k aktivům ve správě CIT, nejmenovité i jmenovité, se ukládají výhradně do administrátorské instance; jejich ukládání do uživatelské instance je zakázáno. Výjimkou je dočasné předání údaje externí osobě funkcí Send podle čl. 7 odst. 2.
3. Sbírky se zakládají podle systémů nebo oblastí správy.

4. Organizace útvarů i sbírky v nich mají určeného odpovědného správce – vedoucího pracoviště či útvaru, který rozhoduje o přístupu k jednotlivým sbírkám.
5. Osobní trezor v uživatelské instanci slouží výhradně k ukládání osobních přístupových údajů zaměstnance, které nejsou administrátorské ani technické. Údaj, který potřebuje i jiná osoba, patří do organizace. Osobní trezor v administrátorské instanci se nepoužívá.
6. Každý zaměstnanec může mít nejvýše jednu osobní organizaci pojmenovanou „Osobní – příjmení“. Do osobní organizace se nezvou další členové a neukládají se do ní nejmenovité údaje. Jiné organizace než organizace útvarů a osobní organizace se nezakládají.
7. Při změně pracovního zařazení nebo ukončení pracovněprávního vztahu zaměstnance odpovědný správce bez zbytečného odkladu upraví nebo odebere jeho přístup ke sbírkám. Hesla ve sbírkách, ke kterým měl zaměstnanec přístup, se změní podle čl. 6 odst. 4. Jmenovité účty, které zaměstnanec v novém zařazení nepotřebuje, se zablokují nebo zruší; při ukončení pracovněprávního vztahu se zablokují nebo zruší všechny jeho jmenovité účty a správce serveru Vaultwarden zruší jeho osobní organizaci. Úkony se evidují v ServiceDesku.

Článek 6
Ukládání záznamů

1. Základní struktura a organizace záznamů ve správci hesel je uvedena v příloze č. 1.
2. Požadavky na hesla jsou uvedeny v příloze č. 3.
3. Při každé změně údaje v systému se bez odkladu aktualizuje i záznam ve Vaultwardenu.
4. Heslo se mění vždy, zejména:
    - při odchodu nebo změně pracovního zařazení osoby, která k němu měla přístup;
    - při podezření na únik nebo kompromitaci (čl. 9);
    - byl-li údaj předán mimo Vaultwarden nebo zobrazen neoprávněné osobě;
    - po použití účtu pro obnovu po incidentu (nouzového účtu);
    - nejméně jednou za 18 měsíců, nevyžaduje-li systém nebo dodavatel kratší interval.

Článek 7
Sdílení

1. Uvnitř CIT se údaje sdílejí výhradně přidělením přístupu ke sbírce v administrátorské instanci https://vw.jcu.cz.
2. S dodavatelem nebo jinou externí osobou se údaje předávají výhradně funkcí Send pomocí instance https://pass.jcu.cz, a to s datem smazání nejvýše 7 dní (u jednorázového přihlášení nejvýše 24 hodin), s počtem zobrazení odpovídajícím počtu příjemců a s ochranou heslem, které se příjemci sdělí jiným kanálem.
3. O předání údaje externí osobě se založí záznam v tiketu ServiceDesku (komu, kdy, k jakému systému a proč); údaj samotný se do tiketu neuvádí.
4. Po ukončení spolupráce nebo smluvního vztahu s dodavatelem se všechny údaje, které mu byly předány, bez zbytečného odkladu změní.

Článek 8
Zabezpečení účtu uživatele

1. Každý uživatel Vaultwardenu je povinen:
   - používat hlavní heslo splňující požadavky podle přílohy č. 3;
   - mít zapnuté vícefaktorové ověření;
   - mít nastaveno automatické zamčení trezoru po nečinnosti nejvýše 60 minut a zamykat trezor při opuštění pracoviště;
   - používat pouze oficiální klienty Bitwarden z oficiálních zdrojů;
   - nepřihlašovat se do Vaultwardenu na cizích, veřejných nebo nespravovaných zařízeních.
2. Export trezoru je dovolen pouze v šifrované podobě chráněné heslem, a to jen pro účely zálohy nebo migrace mezi instancemi.

Článek 9
Podezření na únik či kompromitaci účtu uživatele

1. Zaměstnanec, který zjistí nebo má podezření, že citlivý údaj unikl nebo byl předán mimo Vaultwarden, anebo že byl kompromitován jeho účet ve Vaultwardenu či zařízení s klientem Vaultwardenu, to bez odkladu oznámí manažerovi kybernetické bezpečnosti JU (dále jen „MKB“) a odpovědnému správci a založí incident v ServiceDesku na adrese kyber@sd.jcu.cz.
2. Dotčené údaje se bez odkladu změní. Při podezření na kompromitaci účtu ve Vaultwardenu se změní hlavní heslo, ukončí se všechny aktivní relace a změní se všechny údaje, ke kterým měl účet přístup.

Článek 10
Kontrola a přezkum tohoto opatření

1. Opatření a jeho přílohy se přezkoumávají nejméně jednou ročně a po bezpečnostním incidentu souvisejícím s přístupovými údaji nebo po změně právních předpisů.

Článek 11
Závěrečná ustanovení

1. Toto opatření nabývá platnosti a účinnosti dne 3. 11. 2026.
2. Ustanovení tohoto opatření nezbavují zaměstnance povinností vyplývajících z právních předpisů (např. ZoKB, GDPR) ani z ostatních vnitřních předpisů JU.
3. Přílohy tohoto opatření se aktualizují bez nutnosti vydání nového opatření, vždy se zaznamenáním data verze přílohy.

Eduard Krlín
Digitálně podepsal Eduard Krlín
Datum: 2026.11.02 15:30:34 +01'00'

Bc. Eduard Krlín
ředitel

Centrum informačních technologií
Jihočeská univerzita v Českých Budějovicích

Zpracoval: Robert Kroupa, Centrum informačních technologií JU

Rozdělovník: zaměstnanci CIT JU

Přílohy:

Příloha č. 1 – Základní struktura záznamů ve správci hesel Vaultwarden

Příloha č. 2 – Princip sdílení záznamů ve správci hesel Vaultwarden

Příloha č. 3 – Podoba záznamu ve správci hesel a požadavky na hesla

Příloha č. 4 – Aktuální jmenný seznam správců sbírek