Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-S-004**
Název dokumentu:	**Zásady poskytnutí privilegií vyššího administrátora**
Typ dokumentu:	Směrnice výboru pro řízení kybernetické bezpečnosti JU
Rozsah:	Směrnice je určena pro všechny zaměstnance JU.
Prvek legislativy:	-----
Datum vydání:	01. 03. 2025
Datum účinnosti:	**01. 03. 2025**
Platnost do:	odvolání
Počet stran + příloh:	5 + 0
Verze:	1.0
Význam a benefity:	Význam této směrnice je minimalizovat rizika spojená s nadměrným využíváním administrátorských oprávnění a zavést jasně definovaná pravidla odpovědnosti uživatelů, kteří tato oprávnění využívají. Hlavním cílem celé směrnice je vytvořit přehled a správu nad poskytnutými administrátorskými privilegii.
Uložení:	ISMS část na Wiki JU – wiki.jcu.cz
Ruší dokumenty:	-----
Zpracovatel:	Jan Urbánek - Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační sdělení

Tato směrnice stanovuje pravidla a závazné podmínky pro správu a využívání privilegií vyššího (serverového) administrátora a správce aplikací (dále jen „administrátor“). Pravidla a podmínky se vztahují na všechna zařízení ve vlastnictví JU, do který spadají počítačové stanice, notebooky, servery, síťová zařízení, datová úložiště, virtuální stroje a další specializované systémy (dále jen „zařízení“).

Směrnice slouží k ochraně univerzitní IT infrastruktury, dat a informačních systémů před bezpečnostními hrozbami, které mohou vzniknout zneužitím administrátorských práv, a zároveň k vytvoření přehledu a kontroly nad přidělenými a využívanými administrátorskými právy.

Zaměstnanci, kteří obdrží tato privilegia, mohou provádět zásahy na daném zařízení, od zásadní změny konfigurace systému až po přístup k citlivým datům a mnoho dalších oprávnění. Toto vyžaduje vysokou míru odpovědnosti a dodržování bezpečnostních zásad.

Tyto zásady se vztahují i zpětně na již udělená administrátorská práva. Stávající zaměstnanci s privilegii zažádají o poskytnutí práv nebo jim budou odejmuta.

a) Podmínky pro poskytnutí privilegií administrátora

Každý zaměstnanec, který žádá o administrátorská práva je povinen prostřednictvím ServiceDesk JU podepsat protokol, a to elektronicky nebo v tištěné podobě.

- **Aktivace privilegií serverového administrátora** je vždy vázána na konkrétní zařízení, které zaměstnanec spravuje.
- **Aktivace privilegií správce aplikací** je vždy vázána na konkrétní aplikaci, kterou zaměstnanec spravuje.

Privilegia administrátora budou poskytnuta pouze v případech, kdy je jejich využití nezbytně nutné pro plnění pracovních úkolů nebo správy, které nelze efektivně provádět s běžnými uživatelskými právy.

Informace, které nejsou automaticky doplněné při založení formuláře, vložte do textového pole ve formuláři.

1) **Postup pro součásti s majetkem ve správě aktiv JU**

Zaměstnanci součástí, které evidují svá technická aktiva skrze správu aktiv JU, využijí možnost elektronického podpisu protokolu[1] ve službě ServiceDesk.

Do protokolu pro serverová privilegia doplňte:

- Účet na serveru

[1] Odkaz k návodu pro vystavení protokolu je k dispozici na stránce Wiki této směrnice.

Do protokolu pro privilegia správce aplikací doplňte:

- Účet do aplikace (název a typ přihlášení)
- Roli/role přiřazené k účtu zaměstnance
    - Př.: doménový admin, SafeQ admin, globální správce, …

Oznámení o podepsání protokolu vám přijde na univerzitní e-mail.

Všechny vystavené a podepsané protokoly se žádostmi o administrátorská privilegia jsou dohledatelné v rámci ServiceDesk pod účtem zaměstnance v položce *Mé dokumenty*.

V rámci správy aktiv jsou protokoly provázané v přílohách uživatele a jednotlivých zařízení.

2) Postup pro součásti s majetkem mimo správu aktiv JU

Zaměstnanci součástí, které nevyužívají evidenci svých technických aktiv v rámci správy aktiv JU, musí podepsat protokol bez vazby na majetek[2] vystavený IT oddělení součásti.

- Oznámení o podepsání protokolu vám přijde na univerzitní e-mail.

Tato verze evidence slouží jako dočasné řešení. Po začlenění všech součástí JU do správy aktiv v rámci ServiceDesk bude využíván výhradně postup 1).

Pracovník IT oddělení součásti doplní údaje pro jednoznačnou identifikaci zařízení, na které se uplatňují administrátorská privilegia zaměstnance.

Protokol pro serverová privilegia bude obsahovat:

- Účet na serveru
- Server, na který se práva aplikují (název a typ)

Protokol pro privilegia správce aplikací bude obsahovat:

- Název aplikace
- Účet do aplikace (název a typ přihlášení)
- Roli/role přiřazené k účtu zaměstnance
    - Př.: doménový admin, SafeQ admin, globální správce, …

Všechny vystavené a podepsané protokoly se žádostmi o zvýšená privilegia jsou dohledatelné v rámci ServiceDesk pod účtem zaměstnance v položce *Mé dokumenty*.

V rámci správy aktiv jsou protokoly provázané v přílohách uživatele a jednotlivých zařízení.

[2] Návod pro vystavení protokolu bez vazby na majetek je v rámci stejného odkazu na Wiki JU.

b) Povinnosti zaměstnanců s privilegii administrátora

Zaměstnanci, kterým byla přidělena privilegia administrátora, nesou klíčovou odpovědnost za zajištění bezpečnosti a funkčnosti serverů, služeb a aplikací, které spravují v těchto bodech:

- **Osobní odpovědnost uživatele**

Tato privilegia představují riziko pro univerzitní infrastrukturu. Zaměstnanci nesou plnou odpovědnost za veškeré činnosti, včetně případných škod nebo bezpečnostních incidentů.

Porušení těchto povinností může vést k odebrání administrátorských práv nebo kázeňskému opatření.

- **Aktualizace zařízení a aplikací**

Zaměstnanec zajistí, aby všechna zařízení nebo aplikace, které spravuje, byly pravidelně aktualizovány, zejména pokud se jedná o bezpečnostní záplaty operačního systému, aktualizace softwaru a aplikací běžících na serverech, aktualizace knihoven a další doplňky či služby nezbytné pro jejich správnou funkčnost. Dále je zaměstnanec povinen pravidelně kontrolovat a aktualizovat konfiguraci spravovaných serverů či aplikací.

Pokud je server nebo aplikace mimo oficiální podporu výrobce, kvůli které není možné instalovat nové aktualizace, zaměstnanec musí prozkoumat možnosti migrace služeb na aktuálně podporovanou platformu.

V případě, že migrace není možná a server či aplikace nadále představuje nezbytný prvek pro chod klíčové služby, zaměstnanec je povinen zajistit jeho odizolování od zbytku infrastruktury, pravidelně monitorovat jeho činnost pro podezřelé aktivity a využít dostupné prostředky k dosažení maximální ochrany.

Veškeré kroky pro zajištění izolace a pravidelného monitorování je možné konzultovat s CIT, výborem pro řízení kybernetické bezpečnosti nebo architektem kybernetické bezpečnosti JU.

- **Instalace softwaru**

Aplikace na zařízení a doplňky, či jiné služby, do aplikace lze instalovat pouze z důvěryhodných a oficiálních zdrojů. Zaměstnanec musí věnovat zvýšenou pozornost, aby při instalaci nedošlo k instalaci škodlivého nebo nepotřebného softwaru.

Je zakázáno instalovat software, který není schválen univerzitou, nebo software nelegální, jehož použití může zavléci do systému škodlivý kód a zranitelnosti.

Zaměstnanec nese odpovědnost za zajištění, že instalovaný software nenaruší bezpečnost JU (např. instalace nebezpečného softwaru apod.).

- **Zabezpečení zařízení nebo aplikace**

Zaměstnanci nesmí provádět žádné úpravy, které by mohly oslabit bezpečnostní opatření nebo zavléct zranitelnosti do zařízení a aplikace.

Pokud se administrátor připojuje k zařízení nebo aplikaci vzdáleně, je zakázáno využívat neznámé nebo nezabezpečené bezdrátové sítě a komunikační kanály. Ke vzdálenému

připojení je zaměstnanec povinen využít vždy univerzitní službu VPN nebo předurčený přípojný bod (Jump server).

Zaměstnanec je povinen zajistit, že nedojde k neoprávněnému zpřístupnění zařízení nebo aplikace skrze jeho účet, a to jak fyzicky, tak i vzdáleně pomocí protokolů vzdálených ploch nebo jiných možností jako je například protokol SSH.

- **Zabezpečení účtu**

Každý administrátorský účet musí být chráněn silným heslem. Heslo pro účty s těmito vysokými privilegii musí dodržet heslovou politiku JU.

Pro správu hesel by měl administrátor využít prostředí VaultWarden, dostupné na URL https://vw.jcu.cz.

Doporučení: Pokud je to možné, nainstalujte a využijte vícefaktorovou autentizaci v rámci serverů nebo aplikací. Například Google PAM ve spojení s VaultWarden JU pro servery UNIX, nativní řešení MFA v rámci M365 pro servery Windows nebo integrované MFA řešení dostupné v aplikacích.

- **Sdílení účtu**

Administrátorské účty jsou určeny výhradně pro individuální použití. Přihlašovací údaje k těmto účtům nesmí být sdíleny mezi zaměstnanci nebo jinými osobami.

Pokud je sdílení přístupu nezbytné, například pro zajištění zástupu, musí být realizováno prostřednictvím VaultWarden instance na JU, která umožňuje bezpečné sdílení hesel a další funkce.[3]

- **Dodržování bezpečnostních standardů**

Zaměstnanec musí při práci dodržovat platné předpisy v oblasti kybernetické bezpečnosti a jiných oblastí (např. zákon č. 181/2014 Sb. o kybernetické bezpečnosti, GDPR, interní bezpečnostní politiky JU apod.).

[3] Na sdílení účtů se vztahuje kyberbezpečnostní směrnice pro správu hesel – dostupná na Wiki JU v kategorii ISMS.

d) Postihy a odpovědnost za škody

- **Finanční a právní odpovědnost**

Zaměstnanec, který disponuje administrátorskými privilegii, odpovídá za veškeré škody či způsobené incidenty, které vznikly důsledkem neoprávněného nebo nedbalého využívání těchto privilegií a může vést k odebrání administrátorských oprávnění.