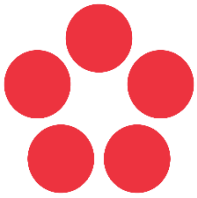

Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-S-003**
Název dokumentu:	**Zásady poskytnutí privilegií lokálního 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:	4 + 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 lokálního administrátora na počítačových stanicích, noteboocích nebo dalších specializovaných systémech, vlastněných JU.

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 privilegia administrátora, získávají oprávnění provádět zásadní změny v konfiguraci systému na dané stanici. 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 lokální administrátorská práva, na jemu přidělené počítačové stanici, notebooku, či jiného zařízení (dále jen „zařízení“), je povinen prostřednictvím ServiceDesk JU podepsat protokol, a to elektronicky nebo v tištěné podobě.

- **Aktivace privilegií lokálního administrátora** je vždy vázána na konkrétní stanici zaměstnance.

V případě předání nového zařízení, ať už novému nebo stávajícímu zaměstnanci, je nutné znovu požádat o přidělení těchto administrátorských práv.

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.

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

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.

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

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 lokální administrátorská privilegia zaměstnance.

Protokol pro lokální privilegia bude obsahovat:

- Druh a název zařízení
- Sériové a inventární číslo

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.

b) Povinnosti zaměstnanců s privilegii lokálního administrátora

Zaměstnanci, kterým byla přidělena privilegia lokálního administrátora nesou zvýšenou odpovědnost za bezpečnost stanice a univerzitní infrastruktury a musí dodržovat zásady v těchto bodech:

- **Osobní odpovědnost uživatele**

Tato privilegia představují riziko pro univerzitní infrastrukturu. Zaměstnanci nesou plnou odpovědnost za veškeré činnosti provedené prostřednictvím stanice spjaté s těmito privilegii, včetně případných škod nebo bezpečnostních incidentů.

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

- **Aktualizace systému a aplikací**

Zaměstnanci jsou povinni udržovat operační systém a všechny aplikace aktuální. Pravidelné aktualizace minimalizují riziko zneužití zranitelností.

Administrátorská práva umožňují upravovat nebo dokonce vypínat aktualizace. Záměrné neprovádění aktualizací je považováno za porušení bezpečnostních zásad.

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

V případě problémů zaměstnanec nestahuje aktualizační balíčky operačního systému nebo aplikací z neznámých zdrojů.

- **Instalace softwaru**

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 stanice**

Zaměstnanci nesmí provádět žádné úpravy, které by mohly oslabit bezpečnostní opatření, například deaktivace firewallu nebo antivirové ochrany.

Je zakázáno se připojovat k neznámým nebo nezabezpečeným bezdrátovým sítím na přenosných zařízeních s administrátorskými privilegii.

Zaměstnanec je povinen zajistit, že nedojde k neoprávněnému zpřístupnění stanice, která disponuje oprávněním lokálního administrátora, a to jak fyzicky, tak i vzdáleně skrze funkci vzdálené plochy nebo jiných možností jako je například protokol SSH.

- **Zabezpečení účtu**

Zaměstnanec s privilegii lokálního administrátora by měl svůj účet chránit silným heslem. Heslo pro účty s těmito vysokými privilegii musí dodržet heslovou politiku JU.

Zaměstnanec nesmí sdílet ani účet s privilegii lokálního admina, ani zařízení, na kterém jsou tato privilegia nastavena, s jinou osobou.

V případě podezření na zcizení přihlašovacích údajů ke svému účtu je zaměstnanec povinen neprodleně si změnit své heslo.

Pro využití privilegií lokálního administrátora je zaměstnanec povinen mít nastavené dvoufázové ověřování na svém univerzitním účtu. Toto je důležité pro zamezení šíření vektorů útoku skrze jeho účet, v případě napadaného zařízení.

- **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.).

- **Provádění neautorizovaného testování bezpečnosti JU**

Jakékoli testování bezpečnosti univerzitních systémů, prováděných ze stanic s privilegii lokálního administrátora (např. penetrační testování, skenování portů, simulace útoků) musí být předem schváleno výborem pro řízení kybernetické bezpečnosti JU.

Neautorizované testování bude považováno za bezpečnostní incident.

c) 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.