Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-008**
Název dokumentu:	**Politika bezpečného chování uživatelů**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Politika se vztahuje na všechny uživatele organizace v kontextu bezpečného nakládání s aktivy, použití hesel, elektronické pošty, sociálních sítí, mobilních zařízení, přístupu na internet a vzdáleného přístupu.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 9, 10, 12, 14
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	3 + 0
Verze:	1.1
Význam a benefity:	Politika určuje základní pravidla bezpečného chování uživatelů na internetu, za účelem zajištění bezpečnosti informací a snížení rizik výskytu kybernetického bezpečnostního incidentu.
Uložení:	Sekce kyberbezpečnosti na Wiki JU
Ruší dokumenty:	-
Zpracovatel:	Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

a) Pravidla pro bezpečné nakládání s aktivy

Každý zaměstnanec zastává výkonem své funkce v organizaci bezpečnostní roli a je povinen aktiva organizace chránit. Zejména:

- dodržovat mlčenlivost,
- pravidelně se vzdělávat a absolvovat testy znalostí,
- pečovat ve své roli o aktivum, se kterým pracuje, a o ostatní aktiva, se kterými přichází do styku (z hledisek zachování jejich dostupnosti, důvěrnosti a integrity),
- dodržovat pracovní postupy a stanovené politiky (ve vztahu k aktivu, uživatelům a dodavatelům),
- vést provozní záznamy a udržovat dokumentaci,
- přihlašovat se v systému přidělenou elektronickou identitou,
- hlásit jakékoliv bezpečnostní události a
- dbát pokynů nadřízeného v provozních a mimořádných situacích.

Všechny dokumenty musí být vypracovány v oficiálních šablonách, které musí obsahovat i označení klasifikace informací. Původce informace je povinen vybrat označení podle příslušné kategorie.

V případě poruchy hardwaru a nutnosti opravy zařízení třetí stranou musí být pevný disk zařízení zálohován na bezpečné úložiště a před předáním externímu technikovi bezpečně vymazán.

Nakládání s aktivy musí být v souladu s Politikou řízení aktiv.

b) Bezpečné použití přístupového hesla

Jednotlivci jsou zodpovědní za bezpečnost a důvěrnost hesel. Pro bezpečné používání hesel se musí dodržovat následující:

- v případě potřeby, hesla k organizačním osobním účtům:
  - nesmí být nikdy sdílena s jinou osobou z jakéhokoli důvodu nebo jakýmkoli způsobem, který není v souladu s touto politikou,
  - nikdy nesmí být zapsána a ponechána na místě snadno přístupném nebo viditelném pro jiné osoby,
  - musí být jedinečná a odlišná od hesel používaných pro jiné osobní účty (např. bankovnictví),
  - musí být měněna při podezření či potvrzení kompromitace,
- výchozí heslo se musí bezodkladně změnit po jeho prvním použití;
- uživatelé nesmí nikdy žádat o heslo někoho jiného;
- osoby s administrátorským přístupem k výpočetní technice musí přístupová hesla k těmto technologickým prostředkům uchovávat v bezpečném správci hesel a zajistit přístup k těmto údajům zastupujícím správcům;
- v případě, že je třeba vydat heslo vzdálenému uživateli nebo poskytovateli služeb, musí být heslo odesláno s náležitými ochrannými opatřeními (např. sdíleno

prostřednictvím zabezpečeného správce hesel nebo odesláno prostřednictvím šifrované e-mailové zprávy);

- osoby s přístupem k servisním nebo testovacím účtům musí zajistit, aby heslo k účtu bylo v souladu s touto politikou, a musí heslo uchovávat v bezpečném správci hesel;
- v případě podezření na narušení nebo kompromitaci musí být incident neprodleně nahlášen.

c) Bezpečné použití elektronické pošty a přístupu na internet

Při používání elektronické pošty se uživatelé musí řídit Politikou bezpečného předávání a výměny informací.

Veškerá odeslána elektronická pošta citlivého původu musí obsahovat i označení klasifikace informací, např. v souladu s metodikou Traffic Light Protocol.

Uživatel musí dbát na bezpečnost informací v souladu s Politikou ochrany před škodlivým kódem.

d) Bezpečný vzdálený přístup

Vzdálený přístup musí být zabezpečen pomocí šifrování (např. pomocí virtuální privátní sítě (VPN)) a silných přístupových hesel (a musí být v souladu s Politikou bezpečného používání kryptografické ochrany a s kapitolou b)).

Při používání počítače ve vlastnictví JU ke vzdálenému připojení k síti JU musí uživatelé zajistit, aby nebyli současně připojeni k žádné jiné síti, s výjimkou osobních sítí, které jsou plně pod jejich kontrolou nebo pod plnou kontrolou třetí strany.

Všechna zařízení, která jsou připojena k síti JU prostřednictvím technologií vzdáleného přístupu, musí používat nejaktuálnější antivirový software.

e) Bezpečné chování na sociálních sítích

Používání cizích sociálních sítí k propagaci organizačních aktivit musí být předem písemně schváleno příslušným vedoucím. Souhlas musí definovat rozsah schválené činnosti, mimo jiné včetně určení oprávněných uživatelů.

Není-li to výslovně povoleno, je zakázáno používat organizační e-mailové adresy na sociálních sítích.

Pověřená osoba musí jménem organizace zkontrolovat a schválit obsah jakéhokoli zveřejnění informací na sociálních sítích.

Uživatelé musí respektovat soukromí zaměstnanců JU a nezveřejňovat žádné identifikační údaje zaměstnanců bez jejich svolení.

Pokud by osobní e-mail, příspěvek nebo jiná elektronická zpráva mohla být považována za oficiální sdělení, musí se uvést prohlášení o vyloučení odpovědnosti.

Uživatelé nesmí používat své osobní účty na sociálních sítích ke služebním účelům, pokud jim k tomu organizace výslovně neudělila souhlas.

f) Bezpečnost ve vztahu k mobilním zařízením

Uživatelé se musí řídit Politikou bezpečného používání mobilních zařízení.

Historie revizí

Historie revizí je uvedena u souboru této politiky na Wiki JU.