Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-005**
Název dokumentu:	**Politika bezpečnosti lidských zdrojů**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Povinnost vstupního a pravidelného školení: • všech uživatelů, • administrátorů, • osob zastávajících bezpečnostní role, • dodavatelů o jejich povinnostech, • formou teoretických i praktických školení, • seznámení je s platnými bezpečnostními politikami, • a kontrolovat jejich dodržování.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 9, 10,12, 14, 20
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	3 + 0
Verze:	1.1
Význam a benefity:	Zvyšování bezpečnostního povědomí v oblasti kybernetické bezpečnosti u všech zaměstnanců, stanovení pravidelných a jednorázových školení, zajištění seznámení dodavatelů s bezpečnostními politikami.
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

Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení

JU musí stanovit **plán rozvoje bezpečnostního povědomí**, v elektronické podobě, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah:

1. poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice a
2. potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role.

Rovněž je nutno:

- určit osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny,
- udržovat seznam osob, které školení absolvovaly,
- zhodnotit účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí.

Plán rozvoje bezpečnostního povědomí musí obsahovat:

- základy kybernetické bezpečnosti,
- popis bezpečnostních rolí a povinností jednotlivých osob,
- seznámení se s bezpečnostními politikami,
- přípravu na případy neobvyklého či podezřelého chování informačního nebo komunikačního systému a způsob hlášení těchto neobvyklých situací.

Způsoby a formy poučení uživatelů

Pro všechny uživatele existuje vstupní a pravidelné školení týkající se základů kybernetické bezpečnosti při nástupu do pracovního poměru, resp. s četností minimálně 1× za 2 roky.

Forma školení e-learning je doplněná o praktické ukázky – podvodný e-mail apod.

Způsoby a formy poučení garantů aktiv

Existuje specifické rozšíření školení pro garanty aktiv. Garant aktiva musí být poučen o jeho klíčových činnostech, jakými jsou:

- odpovědnost za rozsah a způsob použití, zajištění funkčnosti, rozvoje, a bezpečnosti aktiva,
- znalost aktiva, jehož je garantem,
- znalost interních bezpečnostních politik a metodik (například Metodika pro hodnocení aktiv a rizik).

Způsoby a formy poučení administrátorů

Existuje specifické rozšíření školení pro administrátory. Administrátoři jsou poučeni o způsobu a rozsahu použití účtů s privilegovaným přístupem.

Administrátoři serverů a aplikací jsou zodpovědní za správné, bezpečné konfigurace spravovaných systémů a jsou schopni správné nastavení zajistit.

Způsoby a formy poučení osob zastávajících bezpečnostní role

Pro osoby zastávající bezpečnostní role musí JU zajistit pravidelná odborná školení v souladu s plánem rozvoje bezpečnostního povědomí, přičemž vychází z aktuálních potřeb povinné osoby v oblasti kybernetické bezpečnosti.

Osoby zastávající bezpečnostní role musí mít dostatečné znalosti, které vyžaduje jimi zastávaná funkce – viz příloha č. 6 Vyhlášky 82/2018.

Bezpečnostní školení nových zaměstnanců

Součástí nástupu nového zaměstnance je školení v souladu s plánem rozvoje bezpečnostního povědomí. Dle zastávané role je zaměstnanec proškolen také specificky rozšířeným školením určeným pro konkrétní pracovní pozici.

Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací

JU musí zajistit kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů.

V JU existuje disciplinární řízení pro případy porušení bezpečnostní politiky zaměstnancem. Součástí řízení je ověření porušení, které bude řízením řešeno.

Seznámení zaměstnanců s disciplinárním řízením probíhá při úvodním školení zaměstnance. Zaškolení musí být doložitelné.

Disciplinární řízení je řešeno v součinnosti s personálním (nebo dalším) oddělením na základě formálních důkazů. Za účelem spravedlivého jednání a vyřešení porušení je účastníkům řízení poskytnuta odborná a technická podpora.

U smluvních partnerů je oblast sankčních jednání obsažena ve vzájemné smlouvě.

Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice

Pokud u zaměstnance dojde ke změně pracovního místa, je nutné absolvovat specifické školení odpovídající novému pracovnímu místu.

Personální oddělení zodpovídá za proces změny pracovní pozice, a s tím spojených povinnostech zaměstnance, a za proces ukončení vztahu zaměstnance.

Dokumentaci všech aspektů předává na personální oddělení příslušný vedoucí daného zaměstnance. V případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajistí předání odpovědností.

Vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu

Povinnost zaměstnanců a dodavatelů vrátit veškerý majetek, který má hodnotu pro JU před ukončením pracovního vztahu, je součástí pracovní nebo dodavatelské smlouvy.

Tato aktiva spadají do těchto kategorií:

- informace
- dokumentace
- znalosti
- hardware a další majetek

Informace a dokumentace, ať už elektronické nebo papírové – musí být vráceny. Zjištění rozsahu aktiv ke vrácení je součástí ukončovacího pohovoru nebo dodavatelské smlouvy.

Znalosti – dovednosti a kompetence, které může propuštěný zaměstnanec nebo dodavatel mít, jsou v procesu ukončování vztahu posuzovány a vedoucí zaměstnanec posoudí, co bude dále zachováno a co ne.

Hardware a další majetek řeší záznam o přiděleném majetku zaměstnance (spravovaný personálním nebo IT oddělením).

Automatické a neprodlené odebrání přístupových práv bývalým zaměstnancům a partnerům je součástí politiky řízení přístupu.

Změna přístupových oprávnění při změně pracovní pozice

Při změně pracovní pozice zaměstnance, jsou vždy přezkoumána jeho přístupová práva a provedeny případné změny (omezení/rozšíření).

Historie revizí

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