# Jihočeská univerzita v Českých Budějovicích

| | |
|---|---|
| *Označení dokumentu:* | **ISMS-007** |
| *Název dokumentu:* | **Politika řízení přístupu** |
| *Typ dokumentu:* | Interní dokument – **TLP:GREEN** |
| *Rozsah*: | Tato politika se vztahuje na všechny administrátory informačních a komunikačních systémů a osoby zastávající bezpečnostní role. |
| *Prvek legislativy:* | Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 12, 20 |
| *Datum vydání:* | 07. 07. 2026 |
| *Datum účinnosti:* | **07. 07. 2026** |
| *Platnost do:* | odvolání |
| *Počet stran + příloh:* | 2 + 0 |
| *Verze:* | 1.1 |
| *Význam a benefity:* | Tato politika zajišťuje, že přístup k sítím, systémům a datům (dále zdroje) JU mají pouze oprávněné osoby. Pomáhá také chránit aktiva JU před neoprávněným přístupem a zneužitím, a předcházet vnitřním hrozbám, které mohou být způsobeny zaměstnanci nebo dodavateli, kteří mají oprávněný přístup k systémům JU, ale mohou zneužít svá oprávnění. |
| *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) Princip minimálních oprávnění/potřeba znát (need to know)

1. Pro všechny typy účtů musí být uplatněn princip need-to-know. To znamená, že každý účet má nastavena pouze taková oprávnění, která jsou nezbytná pro provádění činností odpovídajících pracovní pozici a náplni práce uživatele. Vedení organizace není výjimkou a má využívat běžné uživatelské účty.

2. Privilegované účty mají přiděleny samostatné přihlašovací údaje. Jednotliví administrátoři musí mít vedle privilegovaného účtu i účet běžného uživatele pro činnosti, které nevyžadují privilegovaná oprávnění.

## b) Požadavky na řízení přístupu

1. Před povolením přístupu ke zdrojům musí být uživatelé autentizováni. To může zahrnovat použití hesla nebo jiných autentizačních metod, jako jsou biometrické údaje nebo tokeny.

2. Pro správu oprávnění přístupu, včetně přidělování a odebírání oprávnění pro jednotlivé uživatele a přístupové skupiny, musí být zaveden proces.

3. Přístupová oprávnění se musí pravidelně přezkoumávat, aby se zajistilo, že jsou stále aktuální a v souladu s potřebami organizace.

## c) Životní cyklus řízení přístupu

1. Přístup ke zdroji vzniká v době, kdy je potřeba. Je nutné, aby žádost o přístup byla schválena určeným vedoucím pracovníkem.

2. Při změně pracovních povinností nebo místa v rámci organizace se musí revidovat oprávnění přístupu a zajistit, že jsou stále v souladu s principem nejmenšího oprávnění.

3. Při ukončení pracovního poměru nebo smlouvy se musí přístup ke zdrojům neprodleně zrušit.

4. V případě, že dojde ke ztrátě nebo krádeži přihlašovacích údajů, je nutné ho co nejdříve resetovat a informovat o tom odpovědné osoby.

5. V případě, že dojde k porušení pravidel řízení přístupu, může být přístup ke zdrojům dočasně omezen nebo zrušen.

## d) Řízení privilegovaných oprávnění

1. Privilegovaná oprávnění se poskytují pouze zaměstnancům, kteří k výkonu své práce nutně potřebují přístup k citlivým zdrojům, a to pouze v nezbytně nutném rozsahu.

2. Musí být oddělen/omezen přístup jednotlivých administrátorů tak, aby jeden člověk nemohl organizaci způsobit fatální škody.

3. Privilegovaná oprávnění musí být pravidelně revidována a kontrolována, aby bylo zajištěno, že jsou stále v souladu s principem minimálních oprávnění.

4. Používání privilegovaných oprávnění musí být monitorováno a zaznamenáváno, aby bylo zajištěno, že je používáno v souladu s těmito pravidly.

5. V případě, že dojde k porušení pravidel řízení přístupu privilegovaných oprávnění, může být přístup k privilegovaným oprávněním dočasně omezen nebo zrušen.

### e) Řízení přístupu pro mimořádné situace

1. V případě mimořádné situace, jako je přírodní katastrofa nebo závažný bezpečnostní incident, může být přístup ke zdrojům omezen nebo zrušen.

2. Omezení nebo zrušení přístupu v mimořádných situacích bude provedeno na základě rozhodnutí odpovědných osob a bude zaměřeno na ochranu zdrojů organizace.

3. V případě, že dojde k omezení nebo zrušení přístupu v mimořádných situacích, budou uživatelé informováni o důvodech a očekávaném trvání těchto opatření.

### f) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách

1. V organizaci musí probíhat pravidelné kontroly rozsahu oprávnění uživatelů a administrátorů, aby se zajistilo, že jsou stále v souladu s potřebami organizace a že nedochází k jejich zneužití.

2. Uživatelé musí být rozděleni do přístupových skupin dle jejich role. Každá skupina musí mít definována oprávnění přístupu, spolu s pravidly pro přidělování uživatelů do dané skupiny.

3. Oprávnění jednotlivých skupin, spolu s pravidly pro přidělování uživatelů do daných skupin musí být pravidelně revidovány a kontrolovány, aby bylo zajištěno, že jsou stále v souladu s těmito pravidly.

## Historie revizí

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