

Bezpečnostní směrnice 1.20

Bezpečná práce s hesly

Tento dokument popisuje opatření, které **MUSÍ** nebo **BY MĚLO** být implementováno pro:

- **Bezpečné použití přístupových hesel.**

1 Bezpečné použití přístupového hesla

Cíl: Zajistit jednoznačnou identifikaci uživatelů v rámci daného aktiva – systému, tj. povolení a logování přístupu přes jednoznačnou autorizaci a autentizaci.

1.1 Používání a monitorování a přístupových hesel

Společnost **MUSÍ** stanovit pravidla pro nastavení formálních požadavků na sílu hesla a délce platnosti v návaznosti na specifika daného aktiva (zejména požadavků na důvěrnost). Detailněji jsou pravidla a postupy definovány ve směrnici XY.

Implementační pokyny:

- 1.1.1 Společnost **MUSÍ** vysvětlit a vynucovat používání adekvátní formu hesel pro:
 - a) Uživatelský přístup,
 - b) Privilegovaný přístup (role jako admin, root, sys).
- 1.1.2 Společnost **MUSÍ** v návaznosti na posouzení rizik, používat vícefaktorovou autentizaci. Například dvoufázové ověření, kdy se uživatel **MUSÍ** prokázat pomocí dvou faktorů (prvním je obvykle uživatelské jméno a heslo, druhým pak například PIN, otisk prstu, snímek sítnice oka, elektronický token a podobně).
- 1.1.3 Uživatel **NESMÍ** přihlašovací údaje, tokeny, PIN, certifikáty sdělovat ani umožňovat využívat jiným osobám.
- 1.1.4 Jakékoliv incidenty v souvislosti s vyjádřením nebo zneužitím hesel **MUSÍ** být neprodleně řešeny.

Příloha A: Interpretace klíčových slov

Klíčové slovo	Interpretace
MUSÍ	Naprostý požadavek (<u>bez výjimek</u>).
NESMÍ	Naprostý zákaz (<u>bez výjimek</u>).
MĚLY BY	Doporučený požadavek, mohou existovat platné důvody pro částečné nebo úplné odchýlení od uvedeného, ale MUSÍ být pochopeny a pečlivě zváženy plné důsledky takového chování <u>dříve</u> , než dojde k volbě odlišného postupu (<u>výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik</u>).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (<u>výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik</u>).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)