Príloha č. 2 Bezpečnostné pravidlá pre zabezpečenie prístupu do IKT prostriedkov ŽSR

Každý zamestnanec tretej strany je povinný držať heslo v maximálnej tajnosti a zabrániť jeho prezradeniu. Zamestnanec tretej strany je zodpovedný za zneužitie svojho užívateľského účtu do IKT prostriedkov ŽSR inou osobou, ktorej poskytol svoje prístupové meno a heslo.

Heslá privilegovaných používateľov tretích strán musia spĺňať nasledované kritéria:

- každé prihlasovacie heslo musí spĺňať požiadavku komplexnosti,
- minimálna dĺžka hesla je 20 znakov,
- heslo musí obsahovať veľké a malé písmená, číslice a špeciálne znaky (minimálne jedno veľké písmeno, minimálne jedno malé písmeno, minimálne jednu číslicu a aspoň jeden špeciálny znak),
- heslo nesmie byť menom, akronymom z mena, iniciálkami, dôležitým dátumom, telefónnym číslom, alebo iným údajom spojeným s používateľom,
- heslo nesmie byť totožné s menom používateľa,
- platnosť hesla v doméne je 90 dní, pred vypršaním platnosti hesla server automaticky žiada používateľa o jeho zmenu,
- zmenené heslo nesmie byť jedným z posledných 24 hesiel v histórii hesiel pre daný účet,
- heslo by sa malo dať zmeniť najviac raz za 1 deň,
- zmenené heslá musia mať zmenené viac ako polovicu znakov oproti pôvodnému heslu. Odporúča sa, aby zmenené heslá mali od pôvodného hesla editačnú vzdialenosť aspoň 7 (t. j. počet operácií vymazania, vloženia alebo prepísania znaku, ktorými sa z pôvodného hesla dá získať nové).
- pri nezmenení hesla po 90 dňoch nebude používateľovi umožnené prihlásiť sa na pracovnú stanicu. Účet sa mu zablokuje a bude si musieť požiadať o zmenu hesla a odblokovanie účtu.

Každý zamestnanec tretej strany je zodpovedný za pravidelnú zmenu svojho hesla, a to v súlade s prijatou politikou hesiel.

Heslá bežných účtov zamestnancov tretích strán musia spĺňať nasledované kritéria:

- minimálna dĺžka hesla je 12 znakov
- heslo musí obsahovať písmena aj číslice
- heslo nesmie byť menom, akronymom z mena, iniciálkami, dôležitým dátumom, telefónnym číslom, alebo iným údajom spojeným s používateľom,
- heslo nesmie byť totožné s menom používateľa,
- zamestnanec tretej strany je povinný meniť heslo minimálne raz za 90 dní,
- pôvodné heslo sa môže opakovať až po použití nastaveného počtu iných hesiel (v závislosti od systému).

Pri narábaní s heslami musia byť dodržane minimálne tieto pravidlá:

- prvotné pridelené heslo do IKT prostriedku ŽSR, musí byť zmenené zamestnancom tretej strany pri prvom prihlásení sa,
- heslo nesmie mať zamestnanec tretej strany poznačené na papieri a uložené v blízkosti pracovnej stanice,
- zamestnanec tretej strany ručí za dôvernosť a ochranu svojich prístupových hesiel a zodpovedá za všetky udalosti a transakcie, ktoré sa uskutočnili v IKT prostriedkoch ŽSR s použitím jeho používateľského mena a hesla,
- heslo sa musí zmeniť hneď po zistení jeho prezradenia,
- v prípade prezradenia prístupového hesla alebo podozrenia na jeho prezradenie je poškodený povinný bezodkladne túto udalosť ohlásiť ako bezpečnostný incident na Servicedesk ŽT (920-2727, servicedesk@zsr.sk) resp. priamo príslušnému koordinátorovi zmluvného vzťahu,
- heslá k privilegovaným účtom musia mať zamestnanci tretích strán uložené a uchovávané v zabezpečených priestoroch pod zámkom,
- zamestnanec tretej strany nesmie podnikať žiadne kroky k získaniu hesiel iných používateľov IKT prostriedkov ŽSR
- Pri vzdialení sa od pracovnej stanice je zamestnanec tretej strany povinný zapnúť šetrič obrazovky chránený prístupovým heslom pomocou kláves (Ctrl-Alt-Del).

Pre privilegované účty platia nasledovné všeobecné zásady:

- na základe technických možností a bezpečnostnej klasifikácie môže byť privilegovaný prístup realizovaný prostredníctvom systému na správu privilegovaných účtov (PAM),
- prístup do PAM musí byť podmienený viacfaktorovým overením používateľa,
- privilegovaný používateľ manažovaný systémom na správu privilegovaných účtov (PAM) s prístupom ku kritickým IS alebo jeho častiam, môžu byť funkciami PAM zaznamenávané činnosti, ktoré vykonáva pri takomto prístupe. Prístup k takýmto záznamom budú mať výlučne poverené osoby ŽSR s cieľom vyšetrovania bezpečnostného incidentu v zmysle § 19 ods. (6) pism. d). a § 19 ods. (6) pism. f). zákona 69/2018 o kybernetickej bezpečnosti.