

RIADENIE PRÍSTUPOVÝCH PRÁV

ČLÁNOK 1 RIADENIE PRÍSTUPU K CITLIVÝM DÁTAM SPRACÚVANÝM V IS

- 1.1 Každý používateľ musí pri prístupe do IS/aplikácie a pri práci s nimi použiť jedinečný identifikátor. Identifikátor nesmie identifikovať pracovnú pozíciu, popisovať používateľovu prácu, identifikovať používateľove právomoci. Zdieľanie identifikátorov pre používateľov je zakázané.
- 1.2 Na pridelenie prístupových oprávnení a príslušných identifikátorov do IS/aplikácií a k informáciám Spoločnosti má nárok každý používateľ, ak to vyplýva z jeho náplne práce a funkčného zaradenia, prípadne poverenia a ak je ich pridelenie schválené v súlade s touto smernicou.
- 1.3 Prístup do IS/aplikácií a k informáciám spoločnosti nemôže byť umožnený bez jednoznačnej identifikácie používateľa. Vytvorenie a prípadná zmena prístupových oprávnení musia byť realizované v súlade s procesmi definovanými v tejto smernici.
- 1.4 Úroveň prístupových oprávnení používateľa musí zodpovedať jeho pracovnej náplni a funkčnému zaradeniu.
- 1.5 Za úroveň a rozsah všetkých prístupových oprávnení používateľa, pri dodržaní princípov „segregation of duties“, „need-to-know principle“, „the least-privilege principle“ a „business needs“, je zodpovedný priamy nadriadený používateľa.
- 1.6 Priamy nadriadený (pre interných zamestnancov), resp. zodpovedná osoba (pre zamestnancov tretích strán) je zodpovedný za vykonanie prehodnotenia úrovne a rozsahu prístupových oprávnení; toto musí byť realizované pri akejkoľvek zmene, ktorá ovplyvní požiadavky na úroveň a rozsah prístupových oprávnení, napr. zmena typového pracovného miesta, zmena pracovnej náplne zamestnanca, zmena predmetu zmluvy a podobne.
- 1.7 Zamestnancom sú prístupové oprávnenia pridelené len na čas, aký si vyžaduje ich pracovná náplň a pracovné zaradenie, najviac však do dňa ukončenia ich pracovného pomeru.

ČLÁNOK 2 PRIDEĽOVANIE PRÍSTUPOVÝCH OPRÁVNENÍ

- 2.1 Prístup do systému musí byť v prvom kroku schválený priamym nadriadeným (v prípade interných zamestnancov Finance & Partners, s.r.o.) alebo zodpovednou osobou (tretie strany), ktorý zároveň zodpovedá za rozsah prístupových oprávnení podľa bodu 1.6.
- 2.2 V prípade schválenia prístupu priamym nadriadeným resp. zodpovednou osobou, schvaľuje prístup vlastník systému/agendy.

ČLÁNOK 3 ZMENA PRÍSTUPOVÝCH OPRÁVNENÍ

- 3.1 V prípade požiadavky na zmenu prístupových oprávnení do IS je potrebné žiadosť schváliť
 - a. priamym nadriadeným (overenie požadovaných oprávnení podľa bodu 1.6),
 - b. b) vlastníkom IS.
- 3.2 V prípade zmeny prístupových oprávnení je potrebné pôvodné oprávnenia odobrať.

ČLÁNOK 4 RUŠENIE PRÍSTUPOVÝCH OPRÁVNENÍ

- 4.1 V prípade riadneho zrušenia pracovného pomeru je potrebné zrušiť všetky existujúce prístupy zamestnanca do IS.
- 4.2 v prípade okamžitého ukončenia pracovného pomeru je potrebné zabezpečiť okamžité zrušenie všetkých prístupov pridelených zamestnancovi.