SLOVENSKÁ AKREDITAČNÁ AGENTÚRA
PRE VYSOKÉ ŠKOLSTVO

VNÚTORNÝ PREDPIS Č. 7/2024

SMERNICA O RIADENÍ PRÍSTUPOV DO INFORMAČNÝCH SYSTÉMOV SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO

V Bratislave 12. decembra 2024

SMERNICA O RIADENÍ PRÍSTUPOV DO INFORMAČNÝCH SYSTÉMOV SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO

Výkonná rada Slovenskej akreditačnej agentúry pre vysoké školstvo (ďalej len „výkonná rada“) schválila dňa 12. decembra 2024 podľa čl. 9 ods. 1 písm. i) Štatútu Slovenskej akreditačnej agentúry pre vysoké školstvo (ďalej len „agentúra“) túto *Smernicu o riadení prístupov do informačných systémov Slovenskej akreditačnej agentúry pre vysoké školstvo* (ďalej len „smernica“).

Článok 1
Úvodné ustanovenia

1. Cieľom riadenia prístupov do informačných systémov agentúry je umožniť používateľom prístup a prácu s dátami spracovávanými v týchto informačných systémoch, a to v rozsahu určenom pracovnými povinnosťami alebo úlohami používateľa, pri súčasnom zabezpečení požiadaviek na kybernetickú bezpečnosť, dôvernosť a integritu systémov a dát.
2. Používatelia informačných systémov agentúry sú jej zamestnanci alebo tretie osoby, pričom sa pravidlá riadenia prístupov pre tieto skupiny aplikujú rovnako.
3. Informačné systémy agentúry sú tvorené softvérovými komponentmi informačno-komunikačných systémov fungujúce na infraštruktúre a hardvérových zariadeniach, ktoré agentúra vlastní alebo využíva na výkon svojej činnosti a podporu svojich procesov.

Článok 2
Vymedzenie pojmov

1. **Administrátorom komunikačnej infraštruktúry** je zamestnanec agentúry, ktorý zodpovedá za administrovanie agendy prístupových práv v technickej (hardvérovej a softvérovej) časti informačno-komunikačnej infraštruktúry agentúry.
1. **Používateľský účet** je súbor prístupových práv, ktoré umožňujú používateľovi vstup do informačných systémov agentúry.
2. **Používateľom** informačných systémov je zamestnanec agentúry alebo tretia osoba (posudzovateľ, poverená osoba za vysokú školu a pod.), ktorá vstupuje do informačných systémov agentúry a/alebo používa zariadenia pripojené k počítačovej sieti agentúry a má vytvorený používateľský účet.
3. **Správcom prístupov a oprávnení** informačných systémov agentúry je poverený zamestnanec, ktorý zodpovedá za správu a evidenciu používateľov a používateľských účtov, ktorá sa vedie v informačno-komunikačnej infraštruktúre agentúry.
4. **Štandardné prístupové právo** je súhrn prístupových práv vecne priradený konkrétnemu pracovnému zaradeniu používateľa v organizačnej štruktúre agentúry a nepodlieha samostatnému schvaľovaniu. Používateľovi sa pridelí a aktivuje po jeho zaradení na príslušnú pracovnú pozíciu a po splnení nevyhnutných predpokladov na prácu s informačnými systémami agentúry (poučenie o ochrane osobných údajov a pod.).
5. **Neštandardné prístupové právo** je súhrn prístupových práv do informačných systémov agentúry, ktoré sa prideľuje konkrétnemu používateľovi a nie je závislé na konkrétnej pracovnej pozícií. Neštandardné prístupové právo sa prideľuje dočasne a je predmetom samostatného schvaľovania pre jednotlivého používateľa na základe písomnej žiadosti.
6. **Administrátorské prístupové** právo je súhrn prístupových práv vysokej (nadradenej) úrovne za účelom administrácie (správy) informačných systémov agentúry alebo plnenia

iných zákonných povinností. Je predmetom samostatného schvaľovania pre používateľa/používateľov a prideľuje ho predseda výkonnej rady agentúry.
7. **Schvaľovateľom prístupových práv** je vedúci kancelárie agentúry, ktorý schvaľuje prístupové práva jednotlivým používateľom informačných systémov agentúry.
8. **Externý systém** je informačný systém, ktorého prevádzkovateľom nie je agentúra (napr. informačný systém Štátnej pokladnice a pod.).

Článok 3
Metodika riadenia prístupových práv

1. Pod **prístupovým právom** sa rozumie možnosť vykonávať aktivity v danom informačnom systéme (napr. vytvoriť, zobraziť, zmeniť súbor a pod.). Riadenie prístupových práv definuje spôsob a postup, ktorým je povolený, zmenený alebo zakázaný prístup do daného informačného systému.
2. Na riadenie prístupových práv do informačných systémov agentúry sa používa štandardná metodika (model) riadenia založený na rolách (Role Based Access Control – RBAC).
3. Používateľ získava štandardné prístupové práva do jednotlivých informačných systémov spravidla pridelením štandardných prístupových rol, ktoré sú priradené pracovnej pozícii v zmysle organizačného poriadku agentúry.
4. Neštandardné prístupové právo sa prideľuje zamestnancovi výnimočne, a to spravidla na obmedzenú dobu a za účelom špecifických aktivít alebo aktivít nepatriacich do bežnej prevádzky agentúry.
5. Definovanie a vytváranie prístupových rol je súčasťou vývoja a implementácie informačných systémov agentúry, a to v dôsledku interných alebo externých zmien v procesoch, alebo je výsledkom požiadavky na zmenu funkcionalít, ktorá sa riadi príslušnými internými predpismi agentúry.

Článok 4
Postup prideľovania prístupových práv a ich evidencia

1. Zamestnancovi sa používateľský účet vytvorí až po podpise pracovnej zmluvy a zaevidovaní zamestnanca do systému.
2. Zamestnancovi sa na základe jeho pracovného zaradenia (organizačný útvar a pracovné miesto) prideľujú štandardné prístupové práva po splnení všetkých podmienok ustanovených týmto predpisom.
3. Zamestnancovi sa prideľujú prístupové práva najviac takého rozsahu, ktoré sú nevyhnutné na plnenie jeho pracovných povinností a úloh vyplývajúcich z opisu pracovnej činnosti uvedeného v pracovnej zmluve – aplikuje sa zásada najnižších privilégií.
4. V prípade tretích osôb – posudzovateľov sa používateľský účet vytvorí po rozhodnutí výkonnej rady o ich zaradení do zoznamu posudzovateľov a zruší po rozhodnutí výkonnej rady o ich vyradení z tohto zoznamu. Pri stanovení rozsahu prístupových práv sa aplikuje zásada najnižších privilégií.
5. V prípade tretích osôb – poverených za vysokú školu sa akceptuje poverenie podpísané štatutárnym orgánom príslušnej vysokej školy. Pri stanovení rozsahu prístupových práv sa aplikuje zásada najnižších privilégií.
6. Neštandardné prístupové práva sa používateľovi môžu prideliť po súhlase vedúceho kancelárie agentúry.
7. Aktiváciu prístupových práv zabezpečuje administrátor komunikačnej infraštruktúry.
8. Prístupové práva môžu zahŕňať aj špeciálne technické prístupové nástroje (token, čipová karta a pod.), bez ktorých prístup nie je možný, a ktoré sa prideľujú vo väzbe na príslušné prístupové práva.

9. Prístupové práva eviduje písomne alebo v príslušných informačných systémoch správca prístupov a oprávnení, administrátor komunikačnej infraštruktúry alebo poverená osoba v závislosti od povahy konkrétneho prístupového práva.

Článok 5
Proces zmeny a odobratie existujúcich prístupových práv

1. V prípade, ak zamestnanec mení v rámci agentúry svoju pracovnú pozíciu, prístupové práva k informačným systémom, ktoré v novej pozícii nebude používať, sa mu odoberú a nové pridelia v súlade s textom tejto smernice.
2. V prípade ukončenia pracovného pomeru zamestnanca sa prístupové práva odoberú bezprostredne v deň skončenia pracovného pomeru, a to ešte pred vystavením výstupného listu.
3. V prípade tretích osôb sa odobratie prístupových práv vykoná bezprostredne po zániku ich mandátu (článok 4 ods. 4 a 5 tejto smernice).
4. Odobratie vybraných prístupových práv sa môže uskutočniť aj na základe žiadosti nadriadeného zamestnanca alebo v dôsledku interného alebo externého auditu prístupových práv (článok 7), prípadne na žiadosť zamestnanca alebo tretej osoby.
5. V prípade pochybností pri zmenách a odobratí prístupových práv rozhoduje vedúci kancelárie.

Článok 6
Práva a povinnosti

1. Používateľ:
   a) má právo na vytvorenie používateľského účtu za účelom vykonávania všetkých činností a úkonov vyplývajúcich z pracovného zaradenia, pracovnej zmluvy a pokynov nadriadeného,
   b) je povinný chrániť svoje prístupové údaje a heslo pred zneužitím a nesmie umožniť inej osobe prístup do jeho používateľského profilu,
   c) je povinný chrániť pred zneužitím pridelené špeciálne technické prístupové nástroje (token, čipová karta a pod.), ktoré musí mať uložené na bezpečnom mieste (uzamykateľná skriňa, trezor a pod.),
   d) zodpovedá za všetky aktivity a úkony, ktoré vykoná v informačných systémoch agentúry,
   e) je povinný pravidelne si meniť prístupové heslo (PIN) v zmysle odporúčaní a pokynov.

2. Administrátor komunikačnej infraštruktúry:
   a) je povinný vykonať všetky aktivity vedúce k zriadeniu používateľského účtu príslušného zamestnanca v definovanom termíne,
   b) navrhuje úpravu štandardných a neštandardných rol a prístupových práv na základe zistení a skúseností z prevádzky informačných systémov agentúry alebo v dôsledku ich zmien, resp. nových funkcionalít,
   c) navrhuje prístupové práva pri vzniku takej pracovnej pozície, pre ktorú nie sú definované štandardné prístupové práva,
   d) aktívne spolupracuje pri audite prístupových práv.

3. Správca prístupov a oprávnení:
   a) administratívne zabezpečuje proces prideľovania a odoberania prístupových práv a eviduje ich v zmysle článku 4 tejto smernice,
   b) navrhuje zmeny, resp. odobratie prístupových práv v prípade ich nevyužívania alebo možnej hrozby ich zneužitia,
   c) aktívne spolupracuje pri audite prístupových práv.

Článok 7
Interný a externý audit prístupových práv

1. Agentúra minimálne jedenkrát v kalendárnom roku uskutoční interný audit (revíziu) prístupov do informačných systémov agentúry.
2. Účelom interného auditu je preveriť dodržiavanie metodiky prideľovania prístupových práv (článok 3), a to najmä zásady najnižších privilégií, a preveriť opodstatnenosť neštandardných prístupových práv, ak tieto boli pridelené.
3. Účelom interného auditu je taktiež preveriť súlad pridelených prístupových práv a rol vo väzbe na vykonané úpravy a zmeny v informačných systémoch agentúry, resp. vo väzbe na ich nové funkcionality.
4. O výsledkoch auditu sa vypracúva interná správa, ktorá obsahuje odporúčania na zmeny a korekcie zistených nedostatkov.
5. Agentúra môže požiadať aj o externý audit prístupových práv, a to samostatne, alebo ako súčasť auditu kybernetickej bezpečnosti systémov agentúry.

Článok 8
Prístupové práva pri zmenách v informačných systémoch

1. Zmeny v informačných systémoch, ktoré predstavujú kvalifikovaný posun v ich funkcionalitách, zmenu ich obsahu alebo rozsahu, môžu viesť k nevyhnutnosti zmeny, resp. štruktúry prístupových práv (rol) jednotlivých požívateľov.
2. Nevyhnutnosť takejto zmeny posúdi vedúci kancelárie, a to priamo alebo na základe interného auditu prístupových práv (článok 7).

Článok 9
Záverečné ustanovenia

1. Táto smernica je záväzná pre všetkých zamestnancov agentúry, ktorí sú povinní ju dodržiavať.
2. Za dodržiavanie ustanovení a postupov tejto smernice je zodpovedný vedúci kancelárie agentúry.
3. Výnimku z tejto smernice môže udeliť len predseda výkonnej rady agentúry, resp. ním poverená osoba.
4. Pokiaľ sa niektoré ustanovenia tejto smernice stanú neplatnými alebo neúčinnými, nie je tým dotknutá platnosť a účinnosť celej smernice.
5. Na situácie neupravené touto smernicou sa primerane použijú ustanovenia súvisiacich všeobecne záväzných predpisov a vnútorných predpisov agentúry.
6. Táto smernica nadobúda účinnosť schválením výkonnou radou agentúry dňa 12. decembra 2024.

V Bratislave dňa 12. decembra 2024

prof. Ing. Robert Redhammer, PhD.
predseda výkonnej rady agentúry