Smernica

o prideľovaní, modifikácií a zrušovaní užívateľských prístupov do informačných systémov s osobnými údajmi

1. Účel

Stanoviť zásady a postupy pri vytváraní, modifikácií a zrušovaní užívateľských prístupov do informačných systémov s osobnými údajmi. Vymedziť právomoci pri schvaľovaní požiadaviek na užívateľské prístupy. Stanoviť postup a kompetencie zamestnancov pri prideľovaní modifikácií a zrušovaní užívateľských prístupov, čím sa umožní prehľadná správa a riadenie užívateľských skupín.

2. Rozsah

Táto smernica sa vzťahuje na všetkých zamestnancov vrátane externých a predpisuje pravidlá prideľovania, modifikácií a zrušovania užívateľských prístupov do informačných systémov prevádzkovateľa.

3. Výklad pojmov

a) Identifikátor prístupu – užívateľské meno, prípadne iný identifikátor (disketa a pod.),
b) Prístup – právo používať informačný systém s osobnými údajmi a pre účel prístupu má každý užívateľ pridelený identifikátor prístupu a heslo,
c) Žiadateľ – zamestnanec,
d) Externý zamestnanec – taký, ktorý vykonáva činnosť pre prevádzkovateľa, nie je v riadnom pracovnom pomere a je zmluvne viazaný s prevádzkovateľom.

4. Všeobecné ustanovenia

Správca siete je povinný mať prehľad o všetkých užívateľoch informačného systému s osobnými údajmi, ich právomociach a o dobe prístupu. Úroveň prístupového práva užívateľa zodpovedá jeho pracovnej náplni, zodpovednosti za osobné údaje a stupňu ochrany osobných údajov prevádzkovateľa. Za návrh úrovne a rozsahu prístupových práv je priamo zodpovedný schvaľovateľ žiadosti o prístup.

5. Právo na vytvorenie a schválenie prístupu

a) Na pridelenie prístupu a identifikátora prístupu do informačného systému s osobnými údajmi v ich elektronickej a písomnej forme má nárok len ten zamestnanec, ktorému to vyplýva z pracovnej zmluvy, funkčného zaradenia, príp. poverenia a náplne práce,
b) Prístup do elektronickej formy informačných systémov s osobnými údajmi má aj externý zamestnanec a zamestnanec zmluvného partnera, ktorý je dodávateľom elektronickej technológie, ak si to vyžaduje jeho činnosť vo vzťahu k prevádzkovateľovi,
c) Schvaľovacie konanie je jednostupňové, pretože žiadosť musí schváliť vždy správca siete.

6. Postup pri prideľovaní prístupu do informačného systému s osobnými údajmi

a) Prideľovanie prístupových hesiel do informačného systému je realizované správcom siete a mení sa podľa požiadaviek,
b) S heslom nesmie prísť do styku iná osoba ako držiteľ prístupu.

7. Používanie a utajenie prístupu

Zamestnanec nesmie používať pridelené prístupové práva na inú činnosť, ako je stanovená jeho pracovnou zmluvou, funkčným zaradením a náplňou práce. Zamestnanec nesmie poskytnúť svoje prístupové práva a identifikátor prístupu inej osobe. V prípade zneužitia hesla alebo jeho poskytnutia inej osobe, je správca siete povinný okamžite znefunkčniť prístupové práva a zmeniť heslo. Zamestnanec, ktorý poskytol heslo inej osobe porušuje pracovnú disciplínu a prevádzkovateľ je povinný voči nemu vyvodiť príslušné dôsledky v zmysle platného Zákonníka práce.

8. Doba platnosti prístupu

Všetky prístupy pre zamestnancov sa prideľujú na takú dobu, ako si to vyžaduje pracovná náplň zamestnanca. Prístupy pre externých zamestnancov alebo zamestnancov zmluvného partnera zabezpečujúceho elektronické vybavenie prevádzkovateľa sa prideľujú na dobu určitú a musia byť zrušené najneskôr v deň ukončenia zmluvného vzťahu.

9. Právo na zrušovanie prístupov

Požiadať o zrušenie prístupu do informačného systému s osobnými údajmi musí zamestnanec osobného oddelenia po skončení potreby prístupu, napr. ukončenie pracovného pomeru, zmena pracovnej náplne a pod. V prípade narušenia alebo podozrenia z narušenia bezpečnosti informačného systému s osobnými údajmi zruší prístup do informačného systému správca siete.

10. Postup pri zrušovaní prístupu

Žiadateľ o zrušenie prístupu doručí svoju žiadosť správcovi siete, príp. ju podá ústne. Ten istý postup platí aj pri zrušení pracovného pomeru zamestnanca.

11. Zmena užívateľských právomocí

V prípade zvýšenia počtu užívateľských právomocí sa postupuje podľa bodu 6 tejto smernice a v prípade zníženia počtu užívateľských právomocí sa postupuje podľa bodu 10 tejto smernice. V žiadosti o zrušenie prístupu sa uvedie daný informačný systém s osobnými údajmi a právomoci, ktoré majú byť zrušené.

12. Zodpovednosť

Ustanovenie tejto smernice sú povinný dodržiavať zamestnanci, ktorí nakladajú s osobnými údajmi. Za kontrolu dodržiavania tejto smernice sú zodpovední štatutárny zástupcovia spoločnosti.

13. Záverečné ustanovenia

Ustanovenia tejto smernice sa primerane použijú aj na informačné systémy ochrany osobných údajov spracovávaných v písomnej forme.
Táto smernica je súčasťou bezpečnostného projektu na ochranu osobných údajov vypracovaného podľa zákona č. 122/2013 Z. z. o ochrane osobných údajov v platnom znení.

Táto smernica nadobúda účinnosť dňom podpisu.

Schválil: Ing. Bc. Zuzana Hervayová
Štatutárny zástupca

Žiadosť
o pridelenie prístupu do informačného systému s osobnými údajmi

Žiadateľ:.....
(priamy nadriadený zamestnanca, ktorý podľa pracovnej zmluvy, funkčného zaradenia a pracovnej náplne má prístup do príslušného informačného systému, meno a priezvisko, funkcia, prípadne zamestnanec)

Žiadam o pridelenie prístupu do:

.....(názov IS)

.....(názov IS) – uviesť všetky systémy, do ktorých má mať prístup

pre elektronickú formu - *áno *nie **pre písomnú formu - *áno *nie**

na dobu trvania pracovného zaradenia

Schvaľovateľ: .....(meno, priezvisko)

Schvaľujem: ***áno** ***nie**

Prístup do informačného systému pridelený dňa:.....

Založené dňa: .....

(*nehodiace sa škrtnite)