Pravidlá na riadenie prístupu tretích strán na Ministerstve financií Slovenskej republiky

Článok 1
Pohyb tretích strán v objekte/priestoroch ministerstva

(1) Zamestnanci tretej strany sú pri vstupe do objektu ministerstva a odchode z objektu ministerstva povinní riadiť sa pokynmi stálej služby.

(2) Do objektu ministerstva môžu zamestnanci tretej strany vstupovať a z neho odchádzať len k tomu určenými vchodmi pre osoby na Štefanovičovej alebo Kýčerského ulici.

Článok 2
Základné povinnosti tretej strany voči ministerstvu pri poskytovaní prác a služieb spojených s naplnením účelu zmluvy, objednávky alebo projektu

(1) Tretia strana sa zaväzuje, že

a) pred začatím činností spojených s naplnením účelu zmluvy, objednávky alebo projektu a pred pridelením prístupových práv potrebných na výkon týchto činností oznámi ministerstvu personálne obsadenie svojho tímu, ktorý bude vykonávať činnosti spojené s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo,

b) bude bezodkladne informovať ministerstvo o všetkých personálnych zmenách vo svojom tíme, ktorý vykonáva činnosti spojené s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo,

c) oboznámi svojich zamestnancov, resp. tretie osoby realizujúce činnosti spojené s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo s bezpečnostnými požiadavkami v rozsahu tejto prílohy a bezpečnostnej politiky MF SR,

d) oboznámi svojich zamestnancov resp. tretie osoby realizujúce činnosti spojené s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo a následne zabezpečí od týchto zamestnancov dodržiavanie povinnosti:

1. ochrany údajov a záväzku mlčanlivosti o údajoch, s ktorými prišli počas výkonu prác na projekte pre ministerstvo do styku, a to aj po ukončení pracovného, resp. služobného pomeru,
2. zachovávať mlčanlivosť o osobných údajoch, s ktorými počas práce na projekte pre ministerstvo prídu do styku, ako aj zákaz ich využitia pre osobnú potrebu, bez súhlasu ministerstva ich nesmie zverejniť, nikomu poskytnúť ani sprístupniť, pričom povinnosť mlčanlivosti trvá aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu k tretej strane; povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, zdokumentovať všetky zásahy do IKT ministerstva podľa pokynov oprávneného zamestnanca za ministerstvo,
3. rešpektovať operatívne pokyny zamestnancov s pridelenými bezpečnostnými rolami na ministerstve a oprávnených zamestnancov počas výkonu práce na projekte pre ministerstvo,
4. rešpektovať autorské práva k materiálom poskytnutým ministerstvom,
5. vrátiť ministerstvu všetky poskytnuté materiály a údaje vrátane elektronických a zlikvidovať všetky ich kópie, ak to nebude zmluvne dohodnuté inak.

e) poskytne potrebnú súčinnosť audítorovi vykonávajúcemu audit IS, ak tento súvisí s výkonom práce na projekte pre ministerstvo,

f) poskytne potrebnú súčinnosť ministerstvu pre prípadný audit svojich IS a IKT, ak tieto súvisia s predmetom plnenia projektu pre ministerstvo,

g) ak predmet projektu súvisí s vývojom a aktualizáciou IS, resp. IKT ministerstva, bude dodržiavať bezpečnostné požiadavky bezpečnostnej politiky ministerstva, platnej bezpečnostnej legislatívy, najmä požiadaviek zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a súvisiaceho výnosu MF SR a nevniesť nepožadované alebo neschválené funkcie do IS ministerstva. Nenaplnenie tejto požiadavky sa bude považovať za porušenie zmluvného vzťahu.

(2) Tretia strana zodpovedá za všetky priame alebo nepriame škody (napr. náklady, ktoré musí ministerstvo vydať, aby sa vrátilo do doby pred vytváraním informačného systému, sankčné pokuty z dôvodu nedodržania termínov, stanovených napr. zákonom alebo sankčné pokuty za to, že dodávané dielo nespĺňa legislatívou stanovené požiadavky), ktoré svojim úmyselným alebo neúmyselným konaním spôsobí a nahradiť ich ministerstvu.

(3) Tretia strana je povinná zaplatiť zmluvnú pokutu vo výške 500,00 € v prípade porušenia podmienok na zabezpečenie informačnej bezpečnosti ministerstva vyplývajúcich z tejto prílohy.

(4) V prípade nevyhnutnosti prístupu tretích strán k projektom obsahujúcim utajované skutočnosti sa postupuje podľa ustanovení zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Článok 3
Povinnosti zamestnancov tretích strán pri riadení prístupu do IS a aplikácií ministerstva

(1) Zamestnanec tretej strany, resp. tretia osoba realizujúca činnosti spojené s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo, je povinný prihlasovať sa do IS a aplikácií pod prideleným prihlasovacím účtom (ID používateľa) a heslom na prístup do tejto aplikácie alebo IS. Zdieľanie účtov je povolené len po písomnej autorizácii bezpečnostným manažérom a to iba v prípadoch, kedy nie je technologicky možné vynútiť iný spôsob prístupu.

(2) Privilegované používateľské účty nesmú byť používané na bežné činnosti nevyžadujúce privilegované oprávnenia.

(3) Zamestnanec tretej strany resp. tretia osoba realizujúca činnosti spojené s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo nesmie na vykonávanie konfigurácií využívať generické a servisné používateľské účty. Výnimku tvorí len ich individuálne použitie, ktoré musí byť vopred písomne schválené manažérom bezpečnosti ministerstva.

(4) Pri práci s heslami je zamestnanec tretej strany povinný dodržiavať nasledovné zásady:

a) pravidlá zmeny hesla do aplikácií v rámci LAN ministerstva upravuje príslušný garant systému a ich dodržiavanie kontroluje administrátor aplikácie,

b) používateľ je povinný dodržiavať tieto všeobecné zásady tvorby hesla pre prístup do LAN ministerstva, podľa ktorých heslo:

1. musí mať dĺžku minimálne 8 znakov,
2. musí sa skladať z veľkých a malých písmen, číselných znakov (NumLock) a iných znakov (napr. veľké písmeno + malé písmeno + číslo a/alebo špeciálny znak),
3. nesmie byť slovníkovým slovom, menom ani názvom,
4. nesmie byť odvodené od osobných údajov používateľa,
5. nesmie byť tvorené priamou postupnosťou klávesov na klávesnici,
6. pri zmene na nové heslo sa musí od pôvodného líšiť najmenej v štyroch znakoch.

(5) Ak to aplikácia alebo IS dovoľuje, musí byť prvotné heslo, ktoré bolo zamestnancovi tretej strany na prístup do tejto aplikácie alebo IS pridelené, pri prvom prihlásení zmenené.

(6) Zamestnanec tretej strany resp. tretia osoba realizujúca činnosti spojené s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo, ručí za dôvernosť a ochranu svojich prístupových hesiel a zodpovedá za všetky udalosti a transakcie, ktoré sa uskutočnili v IS s použitím jeho používateľského mena a hesla.

(7) V prípade podozrenia na prezradenie prístupového hesla resp. v prípade jeho samotného prezradenia musí poškodený zamestnanec tretej strany okamžite informovať oprávneného zamestnanca za ministerstvo resp. príslušného správcu IS a nahlásiť udalosť ako bezpečnostný incident.

(8) Po ukončení práce je zamestnanec tretej strany resp. tretia osoba realizujúca činnosti spojené s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo, povinný znemožniť prístup k aplikáciám a programom a to tak, aby zabránil neoprávnenému prístupu alebo zneužitiu. Táto povinnosť sa nevzťahuje na zamestnanca tretej strany v prípade, ak mu to odôvodnene neumožňuje charakter vykonávaných prác a táto výnimka je písomne schválená manažérom bezpečnosti ministerstva.

(9) Vzdialený prístup dodávateľa a tretích strán v právnom vzťahu k dodávanému dielu do informačných systémov

a ostatného softvéru ministerstva nie je možný. Prístup je možné povoliť iba manažérom bezpečnosti na základe písomnej žiadosti a to len v priestoroch, ktoré sú v správe ministerstva, a to iba s dohľadom na to určeného zamestnanca.

Článok 4
Pripájanie prenosných počítačov a zariadení zamestnancov tretích strán do IS na ministerstve

(1) Prenosné počítače zamestnancov tretích strán resp. tretích osôb v súvislosti s naplnením účelu zmluvy, objednávky alebo projektu ministerstva smú byť pripájané do IS ministerstva len na základe písomného súhlasu manažéra bezpečnosti ministerstva.

(2) Zamestnanec tretej strany resp. tretie osoby realizujúce činnosti spojené s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo, ktorý uchováva na prenosnom počítači/zariadení informácie, ktorých vlastníkom je ministerstvo, je povinný:

a) chrániť ho pred krádežou alebo zneužitím; zamestnanec tretej strany nesmie ponechať prenosný počítač/zariadenie bez dozoru napr. na verejne dostupných miestach, v dopravných prostriedkoch, neuzamknutých kanceláriách a pod.,

b) okamžite hlásiť stratu, prípadne krádež prenosného počítača ako bezpečnostný incident,

c) ak sú na pevnom disku prenosného počítača/zariadenia ukladané informácie zaradené do triedy dôvernosti „INTERNÉ“ alebo „CHRÁNENÉ“, musia byť tieto informácie chránené dodatočným zabezpečovacím prostriedkom, t. j. šifrovaním.

(3) Dostatočnosť použitých šifrovacích prostriedkov posúdi na základe písomnej žiadosti manažér bezpečnosti ministerstva pred povolením uloženia dát na pevný disk prenosného počítača/zariadenia tretej strany.

Článok 5
Používanie elektronickej pošty ministerstva zamestnancami tretích strán

Pri používaní elektronickej pošty je zamestnanec tretej strany povinný dodržiavať tieto zásady:

a) využívať elektronickú poštu iba na účely plnenia služobných alebo pracovných úloh spôsobom a v rozsahu stanovenom týmto IRA,

b) informovať Help Desk o všetkých neočakávaných správach s prílohami od neznámych odosielateľov (mimo ministerstva), ktoré mu boli doručené elektronickou poštou, správy neotvárať - nečítať z dôvodu ohrozenia zavírením a ďalej postupovať podľa pokynov pracovníka Help Desku,

c) nezapĺňať kapacitu elektronickej pošty objemnými dátami v prílohách,

d) po ukončení práce s elektronickou poštou prostredníctvom externého prístupu - Outlook web Access sa používateľovi odporúča odhlásiť sa a zavrieť okno internetového prehliadača,

e) email s prílohami posielaný mimo ministerstva alebo v rámci siete LAN ministerstva nesmie prekročiť povolenú veľkosť; používateľ má mailovú schránku generovanú automatizovaným procesom s pevne stanovenou veľkosťou a bližšie informácie o kapacitách mailov a veľkosti mailových schránok získa u pracovníkov Help Desku.

Článok 6
Riadenie bezpečnostných incidentov

Každý zamestnanec tretej strany resp. tretie osoby realizujúce prácu v súvislosti s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo je povinný zistenie bezpečnostného incidentu alebo podozrenie na bezpečnostný incident bezodkladne nahlásiť na určené kontaktné miesto, ktorým je Help Desk (tel. číslo: +421 2 5958 2400, kl.: 2400, resp. email: helpdesk@mfsr.sk).

Článok 7
Vyšetrovanie bezpečnostných incidentov

(1) Každý zamestnanec tretej strany resp. tretie osoby realizujúce prácu v súvislosti s naplnením účelu zmluvy,

objednávky alebo projektu pre ministerstvo je povinný, pri vyšetrovaní bezpečnostných incidentov zamestnancom alebo zamestnancami ministerstva, poskytnúť potrebnú súčinnosť.

(2) Po vzniku bezpečnostného incidentu nesmie zamestnanec tretej strany resp. tretia osoba realizujúce prácu v súvislosti s naplnením účelu zmluvy, objednávky alebo projektu pre ministerstvo vykonávať akékoľvek aktivity, ktoré by mohli viesť k znehodnoteniu dôkazov alebo k zhoršeniu dôsledkov BI.