Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnostná politika IS
Organizačná a personálna bezpečnosť

Ivan Kopáčik

Máj 2013

KPMG
cutting through complexity™

Agenda

1. Východiská bezpečnostnej politiky
2. Praktický obsah bezpečnostnej politiky
3. Personálna bezpečnosť vo vzťahu k IS

Politika informačnej bezpečnosti - východiská

- Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len „Výnos“)

- Norma ISO/IEC 27002 Pravidlá dobrej praxe manažérstva informačnej bezpečnosti

Výnos §28 písm. a)

Bezpečnostná politika musí obsahovať:

1. Určenie bezpečnostných cieľov povinnej osoby z hľadiska informačnej bezpečnosti.
2. Určenie spôsobov vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania ich dosahovania, spôsobov priebežného hodnotenia ich adekvátnosti a spôsobov kontroly postupov využívaných na ich dosahovanie.
3. Určenie úlohy vedenia povinnej osoby pri zaisťovaní informačnej bezpečnosti a uvedenie vyhlásenia vedenia povinnej osoby o podpore bezpečnostnej politiky povinnej osoby.

Výnos §28 písm. a)

4. Určenie všeobecných a špecifických zodpovedností a povinností v oblasti informačnej bezpečnosti a stanovenie potrebných pozícií pre manažment informačnej bezpečnosti.
5. Určenie povinnosti za zaručenie nenarušenia informačnej bezpečnosti povinnej osoby.
6. Zhodnotenie súladu bezpečnostnej politiky povinnej osoby so všeobecne záväznými právnymi predpismi, vnútornými predpismi povinnej osoby a jej zmluvnými záväzkami.
7. Určenie požiadaviek na informačné systémy verejnej správy, vyplývajúcich zo všeobecne záväzných právnych predpisov, vnútorných predpisov povinnej osoby a jej zmluvných záväzkov, a určenie spôsobu vedenia a aktualizácie dokumentácie o informačných systémoch verejnej správy.

Výnos §28 písm. a)

8. Určenie rozsahu a úrovne ochrany všetkých informačných systémov verejnej správy vrátane hodnotenia slabých miest a ohrození.
9. Určenie rámca pre manažment rizík u povinnej osoby v súvislosti s aktívami, od ktorých závisí činnosť informačných systémov verejnej správy alebo ktoré závisia od činnosti informačných systémov verejnej správy; rámec najmä určí, ktoré aktíva sú pre povinnú osobu kritické, čo ich ohrozuje, a zásady ich ochrany,
10. Určenie rozsahu a periodicity auditu informačnej bezpečnosti u povinnej osoby a zároveň určenie udalosti v informačných systémoch verejnej správy, o ktorých sa vytvára záznam auditu.
11. Určenie operačných smerníc na zálohovanie a určenie, ktoré skupiny údajov, v akom rozsahu, akým spôsobom a s akou periodicitou sa zálohujú v prevádzkovej zálohe a archivačnej zálohe.

Výnos §28 písm. a)

12. Určenie periodicity monitorovania bezpečnosti a aktualizácie softvéru.
13. Určenie dokumentov, ktoré povinná osoba na zaistenie informačnej bezpečnosti vypracuje a uvedie ich zoznam.
14. určenie postupu pri revízii bezpečnostnej politiky povinnej osoby vrátane periodicity pravidelných revízií a dôvodov mimoriadnych revízií bezpečnostnej politiky povinnej osoby.

Súvisiaca bezpečnostná dokumentácia

Bezpečnostná politika je vrcholový, strategický a kompetenčný dokument („zákon“).

Bezpečnostná politika sa rozpracúva a konkretizuje v interných štandardoch a aktoch riadenia („vykonávacie predpisy“).

Výnos §29 písm. f)

Štandardom pre personálnu bezpečnosť je vypracovanie postupu pri ukončení pracovného pomeru vlastného zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou.

Výnos §30 písm. f)

Štandardom pre manažment rizík pre oblasť informačnej bezpečnosti je vypracovanie plánov na obnovu činnosti nefunkčných, poškodených alebo zničených kritických informačných systémov verejnej správy.

Výnos §33 písm. b), c)

Štandardom pre sieťovú bezpečnosť je:

1. vedenie evidencie o všetkých miestach prepojenia sietí v správe povinnej osoby vrátane prepojení s externými sieťami. (písm. b))
2. zabezpečenie, aby pre každé prepojenie podľa písm. b) bol vypracovaný interný akt riadenia prístupu medzi týmito sieťami podľa §40 riadenie prístupu. (písm. c))

Výnos §34 písm. d)

Štandardom pre fyzickú bezpečnosť a bezpečnosť prostredia je vypracovanie a implementácia pravidiel na prácu v zabezpečenom priestore.

Výnos §34 písm. h)

Štandardom pre fyzickú bezpečnosť a bezpečnosť prostredia je vypracovanie, zavedenie a kontrola dodržiavania pravidiel na:

1. údržbu, uchovávanie a evidenciu technických komponentov informačného systému verejnej správy a zariadení informačného systému verejnej správy,
2. používanie zariadení informačného systému verejnej správy na iné účely, na aké boli pôvodne určené,
3. používanie zariadení informačného systému verejnej správy mimo určených priestorov,
4. vymazávanie, vyraďovanie a likvidovanie zariadení informačného systému verejnej správy a všetkých typov relevantných záloh,
5. prenos technických komponentov informačného systému verejnej správy alebo zariadení informačného systému verejnej správy mimo priestorov povinnej osoby,
6. narábanie s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačného systému verejnej správy tak, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.

Výnos §36 písm. a)

Štandardom pre monitorovanie a manažment bezpečnostných incidentov je vypracovanie interného aktu obsahujúceho:

1. postup pri ohlasovaní bezpečnostných incidentov a odhalených slabých miest informačných systémov verejnej správy, najmä na účel včasného prijatia preventívnych a nápravných opatrení,
2. postup pri riešení jednotlivých typov bezpečnostných incidentov a spôsob ich vyhodnocovania,
3. spôsob evidencie bezpečnostných incidentov a použitých riešení.

Výnos §40 písm. b), j)

Štandardom pre riadenie prístupu je:

a) vypracovanie interného aktu riadenia prístupu k údajom a funkciám informačného systému verejnej správy založeného na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh. (písm. b))

b) vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačného systému verejnej správy. (písm. j))

Výnos §41 písm. e)

Štandardom pre aktualizáciu informačno-komunikačných technológií je uchovávanie a aktualizácia dokumentácie o informačných systémoch verejnej správy alebo ich častiach, ktorá obsahuje:

1. používateľskú dokumentáciu, ktorou je návod na používanie informačného systému verejnej správy,
2. administrátorskú dokumentáciu, ktorou je návod na správu a prevádzku informačného systému verejnej správy,
3. prevádzkovú dokumentáciu, ktorou je dokumentácia o architektúre informačného systému verejnej správy alebo jeho časti, jeho konfigurácii a väzbách na existujúce informačné systémy verejnej správy.

ISO/IEC 27002

Hlavným cieľom je poskytnúť usmernenie pre riadenie a podporu informačnej bezpečnosti v súlade s požiadavkami / potrebami organizácie a relevantnými zákonmi a nariadeniami.

„Manažment by mal prostredníctvom vydania a udržiavania politiky informačnej bezpečnosti v rámci organizácie určiť jasný smer politiky v súlade so svojimi cieľmi a demonštrovať svoju podporu a angažovanosť z hľadiska informačnej bezpečnosti.“

ISO/IEC 27002

Dokument bezpečnostnej politiky by mal byť schválený manažmentom, vydaný a oznámený všetkým zamestnancom, ako aj relevantným externým partnerom.

Dokument politiky by mal obsahovať:

a) definíciu informačnej bezpečnosti, jej celkové ciele, účel a dôležitosť bezpečnosti ako mechanizmu umožňujúceho spoločné používanie informácií,

b) vyhlásenie zámerov manažmentu, podpory cieľov a princípov informačnej bezpečnosti v súlade so stratégiou organizácie a cieľmi,

c) rámec na nastavenie cieľov riadenia a opatrení, vrátane štruktúry preskúmavania rizík a riadenia rizík,

ISO/IEC 27002

d) stručné vysvetlenie bezpečnostných politík, princípov, štandardov a zhody s požiadavkami, dodržiavanie, ktorých má pre organizáciu zvláštnu dôležitosť, napr.:

1. dodržiavanie legislatívnych, regulačných a zmluvných požiadaviek,
2. požiadavky na bezpečnostné vzdelávanie, zácvik a budovanie bezpečnostného povedomia,
3. riadenie kontinuity činnosti organizácie,
4. následky porušení bezpečnostnej politiky.

e) definíciu všeobecných a špecifických zodpovedností z hľadiska manažmentu informačnej bezpečnosti, vrátane ohlasovania bezpečnostných incidentov,

ISO/IEC 27002

f) odkazy na dokumentáciu, podporujúcu danú politiku, napr. detailnejšie bezpečnostné pravidlá a postupy pre špecifické informačné systémy alebo bezpečnostné pravidlá, ktoré by mali používatelia dodržiavať.

S bezpečnostnou politikou by mali byť oboznámení používatelia v rámci celej organizácie, a to formou, ktorá je dostupná a pochopiteľná pre očakávaného čitateľa.

ISO/IEC 27002

Preskúmanie politiky informačnej bezpečnosti

„Politika informačnej bezpečnosti by mala byť preskúmavaná v plánovaných intervaloch, ako aj okamžite pri výskyte významných zmien, čím sa zabezpečí jej kontinuálna vhodnosť, primeranosť a efektivita.“

- Politika informačnej bezpečnosti by mala mať vlastníka, ktorý akceptoval manažérsku zodpovednosť za jej vývoj, revíziu a vyhodnocovanie efektivity
- Preskúmanie by malo zahŕňať ohodnotenie príležitostí na zlepšenie politiky informačnej bezpečnosti organizácie, ako aj postoj k riadeniu informačnej bezpečnosti vzhľadom na zmeny v prostredí organizácie, zákonných podmienok a technickom prostredí
- Preskúmanie politiky informačnej bezpečnosti by malo brať do úvahy výsledky predchádzajúcich preskúmaní manažmentom

ISO/IEC 27002

Vstupy na realizáciu preskúmavania:

a) spätná väzba od zainteresovaných strán,
b) výsledky nezávislých revízií,
c) stav preventívnych a nápravných činností,
d) výsledky predošlých preskúmaní manažmentom,
e) prevádzková výkonnosť a primeranosť politiky informačnej bezpečnosti,
f) zmeny, ktoré môžu mať vplyv na prístup organizácie k riadeniu informačnej bezpečnosti, vrátane zmien prostredia organizácie, obchodných podmienok, dostupnosti zdrojov, zmluvných, regulačných a legislatívnych podmienok, prípadne technického prostredia,
g) trendy vzťahujúce sa na hrozby a zraniteľnosti,
h) nahlásené incidenty informačnej bezpečnosti,
i) odporúčania poskytnuté relevantnými subjektmi.

ISO/IEC 27002

Výstup z preskúmaní manažmentom by mal zahŕňať všetky rozhodnutia a kroky v spojitosti so:

a) zlepšením prístupu organizácie k riadeniu informačnej bezpečnosti a jej procesov,
b) zlepšením cieľov riadenia a opatrení,
c) zlepšením v oblasti alokácie zdrojov a/alebo zodpovedností.

Toľko teória....a teraz prax

Bezpečnostná politika IS v praxi

Úprava zásad, kompetencií, zodpovedností, povinností a opatrení na implementáciu a využívanie bezpečnostnej politiky.

Rozsah: bezpečnostná politika sa vzťahuje na všetky aktíva tvoriace informačný systém organizácie vrátane všetkých aplikácií, dát, elektronických služieb a komunikačnej infraštruktúry.

Typické bezpečnostné ciele organizácie štátnej správy

Dodržiavanie všeobecne záväzných právnych predpisov a požiadaviek relevantných pre oblasť informačnej bezpečnosti.

Minimalizácia finančných a iných strát súvisiacich s narušením prevádzky informačného systému organizácie.

Vytvorenie a prevádzkovanie dôveryhodných a spoľahlivých informačných systémov pre zamestnancov organizácie.

Minimalizácia rizík ohrozenia aktív informačného systému.

Zaistenie poskytovania služieb informačného systému užívateľom informačného systému v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch informačného systému.

Ochrana dobrého mena organizácie.

Spôsoby dosahovania bezpečnostných cieľov – typické princípy

Na ochranu informácií sa vytvoria zodpovedajúce technické a organizačné predpoklady, ktoré sa skonkretizujú v záväzných dokumentoch nadväzujúcich na bezpečnostnú politiku, v bezpečnostných projektoch pre jednotlivé IS a ďalších interných predpisoch organizácie.

Informácie uložené a spravované v informačnom systéme je dovolené spracúvať iba prostredníctvom aplikačného programového vybavenia, ktoré zodpovedá platným štandardom používaným v organizácii.

Pre všetky informačné systémy, ktoré zabezpečujú kontinuálnu činnosť organizácie, sa vypracujú a priebežne aktualizujú havarijné plány.

Účinnosť bezpečnostných opatrení slúžiacich k ochrane informačného systému sa pravidelne kontroluje a vyhodnocuje.

Spôsoby dosahovania bezpečnostných cieľov typické princípy II.

Implementácia nových a rozvoj existujúcich bezpečnostných opatrení sú plánované a koordinované aktivity.

Riešenie informačnej bezpečnosti je súčasťou každého nového projektu, súvisiaceho s ľubovoľným IS (existujúcim alebo novým).

Úroveň bezpečnostného povedomia všetkých zamestnancov organizácie sa pravidelne rozvíja v súlade s cieľmi bezpečnostnej politiky.

Zásady bezpečnostnej politiky sa v relevantnej miere aplikujú aj na tretie strany (napr. dodávateľské firmy a ich zamestnanci).

Potreba priradenia kľúčových zodpovedností

Vypracovanie, aktualizácia a koordinácia uplatňovania bezpečnostnej politiky.

Definovanie a aktualizácia bezpečnostných štandardov organizácie resp. ich prevzatie.

Metodické riadenie organizačných útvarov v oblasti informačnej bezpečnosti.

Koordinácia činností pri analýze a riadení rizík IS a schvaľovaní prvkov IS z hľadiska plnenia bezpečnostných požiadaviek.

Vyhodnocovanie bezpečnostných prvkov prevádzkovaných v IS a posudzovanie požiadaviek na nové IS z hľadiska ich bezpečnosti.

Zabezpečenie školení zamestnancov v oblasti informačnej bezpečnosti.

Koordinácia činností pri prešetrovaní a zvládaní bezpečnostných incidentov.

Sledovanie dodržiavania bezpečnostných opatrení.

Monitorovanie a koordinácia vyhodnocovania záznamov o prístupoch k údajom.

Implementácia a správa systémov ochrany IS.

Potreba priradenia kľúčových zodpovedností II.

Realizácia a koordinácia projektov na zvýšenie informačnej bezpečnosti.

Riadenie prístupu užívateľov IS k aplikáciám.

Monitorovanie a vyhodnocovanie neoprávnených prístupov/pokusov o prístup do IS.

Akceptačné testovanie, schvaľovanie prvkov IS z hľadiska plnenia bezpečnostných požiadaviek.

Spracovanie a vedenie prehľadu o realizovaných riešeniach a opatreniach z oblasti bezpečnosti IS.

Kontrola dodržiavania pracovných postupov v IS.

Zabezpečenie odstraňovania havarijných stavov a bezpečnostných incidentov vrátane ich dôsledkov.

Vývoj APV pri dodržaní bezpečnostných opatrení.

...a kto to bude robiť? SATO ? Niekto ?

Systém riadenia informačnej bezpečnosti (samostatná téma).

Bezpečnostný manažér, bezpečnostný správca, vlastníci aktív/gestori IS, komisia pre informačnú bezpečnosť v organizácii, útvar IT / technický prevádzkovateľ, nadriadený/podriadený, externé firmy, ...

Dôležité je stanoviť ZMYSLUPLNÉ, REALISTICKÉ a DOSIAHNUTEĽNÉ bezpečnostné ciele.

Ešte dôležitejšie je zriadiť a personálne pokryť pracovné miesta / roly, ktoré pomôžu bezpečnostné ciele naplniť.

Gestor IS / vlastník

Poverený pracovník alebo útvar organizácie, ktorý koordinuje a metodicky riadi IS, stanovuje a zodpovedá za požadovanú funkcionalitu IS.

V praxi zodpovedá najmä za:

- definovanie požiadaviek na bezpečnosť aplikácie / IS a požiadaviek na ochranu údajov,
- klasifikáciu údajov a IS organizácie z hľadiska ich citlivosti a definovanie požiadaviek na bezpečnosť ako jednej z funkcionalít pri tvorbe aplikácie a pri jej zmenách,
- definovanie požiadaviek na riadenie a kontrolu prístupu k spracovaným údajom a službám IS,
- vymedzenie a odsúhlasovanie prístupových oprávnení do jeho IS a evidenciu udelených oprávnení,
- definovanie kritických kombinácií prístupových práv,
- definovanie požiadaviek na zmeny v aplikáciách / IS a akceptáciu úplnosti a správnosti vykonaných zmien.

Technický prevádzkovateľ

Správa IKT z hľadiska bezpečnosti plní priame aj nepriame úlohy.

Používanie programových prostriedkov v súlade s licenčnými požiadavkami.

Zabezpečenie správnej, bezporuchovej funkčnosti a systémovej podpory IS.

Implementácia a prevádzkovanie antivírusových prostriedkov.

Spracovanie, pravidelné revidovanie a testovanie plánu obnovy činnosti IS.

Vedenie evidencie všetkých problémov a použitých riešení.

Nadriadený / podriadený

Nadriadený v rozsahu pôsobnosti ním riadeného útvaru:

- zabezpečenie oboznámenia svojich podriadených s ich povinnosťami a zodpovednosťou z hľadiska bezpečnosti IS,
- definovanie požiadaviek na prístupové práva do aplikácií IS pre svojich podriadených v rozsahu ich pracovných povinností a vedenie evidencie o požiadavkách,
- oznamovanie podozrení z narušenia bezpečnosti IS, podozrení z nesprávnej funkcionality IS alebo dostupnosti údajov pre okruh zamestnancov, ktorým tieto údaje nie sú určené alebo narušenia dôvernosti, integrity a dostupnosti údajov a služieb IS.

Používateľ

Používateľ IS zodpovedá za:

- ochranu údajov, ktoré vytvára, spracúva, prijíma, ku ktorým pristupuje alebo kontroluje,
- ochranu pridelených autentizačných údajov a prostriedkov,
- dodržiavanie platných bezpečnostných zásad v potrebnom rozsahu na bezpečné využívanie IS a spracovanie údajov na základe preukázateľného dôvodu oprávňujúceho na prístup do IS,
- bezodkladné oznámenie podozrenia z narušenia bezpečnosti IS (svojmu nadriadenému),
- oznámenie podozrenia z nesprávnej funkcionality využívaného IS alebo dostupnosti údajov pre okruh zamestnancov, ktorým tieto údaje nie sú určené, svojmu nadriadenému,
- správne využívanie zabudovaných bezpečnostných mechanizmov IS.

Organizácia bezpečnosti IS

Cieľom organizácie bezpečnosti IS je kontinuálne a efektívne riadiť informačnú bezpečnosť vrátane vzťahov k tretím stranám a servisným alebo dodávateľským partnerom.

Pre všetky významné IS sa zavedie proces riadenia rizík vykonávaný najmä prostredníctvom analýzy rizík a návrhu bezpečnostných opatrení na zmiernenie identifikovaných rizík na prijateľnú úroveň.

Všetky rozhodnutia o prijatí alebo neprijatí bezpečnostných opatrení sú založené na výsledkoch príslušnej analýzy rizík.

Analýza rizík musí byť primerane formalizovaná, ale nič sa nemá preháňať.

Dôležitá je definícia kľúčových prvkov riadenia informačnej bezpečnosti.

Zodpovednosti za informačnú bezpečnosť v zmluvných vzťahoch s tretími stranami, servisnými alebo dodávateľskými partnermi sa explicitne vymedzujú.

Klasifikácia a riadenie aktív IS

Cieľ je udržiavať adekvátnu ochranu aktív IS podľa ich hodnoty pre organizáciu.

Všetky kritické aktíva IS majú priradeného vlastníka a vedie sa ich evidencia; vlastníkom kritických aktív môže byť rola, funkčné miesto alebo organizačný útvar.

Klasifikačná schéma vymedzí požiadavky na ochranu informačných aktív (napríklad osobné údaje, utajované skutočnosti, citlivé informácie, verejné informácie).

Za klasifikáciu informačných aktív podľa tejto schémy a definovanie požiadaviek na ochranu NIEKTO zodpovedá.

Personálna bezpečnosť vo vzťahu k IS

Potrebujeme redukovať riziká súvisiace s ľudskými chybami, zlyhaniami, zneužitím práv, vedomými alebo nevedomými porušovaniami bezpečnostných zásad.

§ 29 Personálna bezpečnosť (Výnos)

Okrem požiadaviek Výnosu...

- Zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme
- Zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov
- Zákon č. 311/2001 Z. z. Zákonník práce

Obsahujú podmienky pracovno-právnych vzťahov, upravujú aj niektoré aspekty personálnej bezpečnosti:

- predpoklady a podmienky prijatia do štátnej služby, resp. výkonu práce vo verejnom záujme – previerka,
- práva a povinnosti zamestnanca ako aj zamestnávateľa,
- prehlbovanie a zvyšovanie kvalifikácie zamestnancov,
- základné zásady pri porušení pracovnej disciplíny,
- podmienky a povinnosti pri skončení pracovného pomeru.

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Zlyhanie ľudského faktora

Neúmyselné

- nedostatočne zabezpečené heslo
- strata nosičov s dátami, dôležitých dokumentov
- neúmyselné prezradenie citlivých informácií
- ignorovanie varovných signálov IS...

Úmyselné

- úmyselné prezradenie citlivých dát (prístupové heslá, nastavenia systému...)
- poskytnutie osobných údajov tretej osobe
- ukradnutie dôležitého aktíva
- poškodenie alebo obmedzenie prevádzky...

Dôsledky

- strata citlivých dát
- priama alebo nepriama finačná strata
- strata dobrého mena organizácie..

KPMG cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť ľudských zdrojov

Pred nástupom do zamestnania

Počas zamestnania

Ukončenie alebo zmena počas zamestnania

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť ľudských zdrojov pred nástupom do zamestnania

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

Ciele

EFQM
Recognised for excellence
5 star - 2012

Zabezpečiť, že zamestnanci aj tretie strany porozumejú svojim zodpovednostiam a že sú vhodní na výkon rolí, ktoré im budú pridelené.

Bezpečnostné zodpovednosti by mali byť adresované už na úrovni náboru/prijímania pracovníkov a zahrnuté v primeranom opise práce a podmienkach pre pracovnú pozíciu.

Potenciálni zamestnanci, zmluvní partneri alebo používatelia v pozícii tretích strán by mali byť primerane preverení.

Všetci zamestnanci, zmluvní partneri a používatelia v pozícií tretích strán by mali mať podpísané zmluvy stanovujúce ich zodpovednosti počas trvania pracovnoprávneho vzťahu.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prijímacie konanie - proces preverovania

Požiadavka na vykonanie previerky personálneho pozadia všetkých uchádzačov o zamestnanie v súlade s:

- príslušnými zákonmi a právnymi nariadeniami,
- požiadavkami organizácie,
- etikou,
- klasifikačným stupňom infomácií, ku ktorým sa bude pristupovať,
- vnímanými rizikami súvisiacimi s danou pozíciou.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prijímacie konanie - proces preverovania

Pri procese prijímania sa musí podľa požiadaviek kladených na jednotlivé voľné pracovné pozície uskutočňovať previerka, ktorá zahŕňa:

- kontrolu životopisu uchádzača s ohľadom na úplnosť a presnosť,
- overenia proklamovaného vzdelania dokladom o dosiahnutom stupni vzdelania,
- overenie kvalifikačných predpokladov potrebných pre výkon danej pracovnej pozície (relevantné pracovné skúsenosti, doklady o absolvovaní školení, certifikáty a pod.),

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prijímacie konanie - proces preverovania

- posúdenie osobnostných predpokladov na výkon danej pozície,
- kontrolu bezúhonnosti na základe výpisu z registra trestov nie staršieho ako tri mesiace,
- posúdenie a overenie relevantných referencií uchádzačov,
- vyžiadanie informácií o iných pracovných aktivitách podobného zamerania,
- predloženie dokladu o zdravotnej spôsobilosti (ak to povaha pozície vyžaduje).

KPMG
cutting through complexity™

Zmluva, pracovná náplň a podmienky

- zodpovednosti za zachovanie dôvernosti a neprezradenie informácií ešte pred samotným získaním prístupu k prostriedkom spracujúcim informácie,
- zodpovednosti mimo lokality organizácie a mimo štandardný pracovný čas, napr. pri práci z domu,
- kroky v prípade nedodržania bezpečnostných požiadaviek organizácie,
- zaručenie právnych zodpovedností a nárokov zamestnancov a tretích strán napr. v súvislosti so zákonmi na ochranu autorských práv, osobných údajov atď.,
- zodpovednosti za manipuláciu s informáciami prijatými od tretích strán.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť ľudských zdrojov počas zamestnania

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Ciele

Zabezpečiť, že zamestnanci, zmluvní partneri a používatelia v pozícii tretích strán sú si vedomí hrozieb informačnej bezpečnosti, ich zodpovednosti a záväzkov a že sú pripravení dodržiavať a podporovať bezpečnostnú politiku v priebehu ich každodennej činnosti, ako aj znižovať riziká ľudskej chyby.

Personálna bezpečnosť má byť uplatňovaná počas celého obdobia zamestnania jednotlivca v organizácii.

Primeraná úroveň vzdelávania a školenia v oblasti bezpečnostných postupov a správneho používania prostriedkov na spracúvanie informácií by mali byť poskytnuté všetkým zamestnancom ako i tretím stranám, čím sa minimalizujú bezpečnostné riziká.

Mal by byť zavedený formálny disciplinárny proces riešenia narušení bezpečnosti.

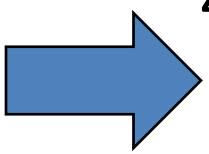
KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

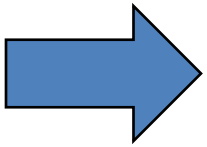
Manažérske zodpovednosti

Neznalosť bezpečnostných zodpovedností zamestnancov



Zvýšené riziko spôsobenia škody, incidentu

Motivovaný, upovedomený personál



Tendencia byť spoľahlivý, nebyť príčinou incidentu

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Manažérske zodpovednosti

Povinnosť manažmentu vyžadovať uplatňovanie informačnej bezpečnosti od:

- zamestnancov,
- zmluvných partnerov,
- používateľov v pozícii tretích strán.

KPMG
cutting through complexity™

Manažérske zodpovednosti

- oboznámenie zamestnancov o rolách a zodpovednostiach spojených s informačnou bezpečnosťou ešte pred prístupom k citlivým informáciám a IS,
- poskytnutie aktuálnych riadiacich aktov pojednávajúcich o bezpečnostných rolách,
- motivácia k napĺňaniu bezpečnostných smerníc organizácie,
- zvyšovanie povedomia o informačnej bezpečnosti,
- udržiavanie dostatočných zručností a kvalifikácie.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť

Cieľom je umožniť rozpoznať problémy a incidenty v informačnej bezpečnosti a reagovať primerane vzhľadom na svoje pracovné zaradenie.

Všetci zamestnanci organizácie by mali absolvovať periodické školenia za účelom udržiavania bezpečnostného povedomia a mali by im byť poskytované aktuálne verzie politík a smerníc organizácie, ak si to vyžaduje ich pracovné zaradenie.

KPMG
cutting through complexity™

Bezpečnostné povedomie, vzdelávanie a školiaca činnosť by mali:

- byť primerané a vhodné pre rolu a zodpovednosti jednotlivca,
- objasniť požiadavky a očakávania organizácie pred udelením prístupu k informáciám alebo službám IS,
- objasniť právnu zodpovednosť zamestnancov za ich konanie,
- sprostredkovať zácvik v správnom používaní prostriedkov na spracovanie informácií podľa zaradenia zamestnanca,
- zahŕňať primerané informácie o známych hrozbách,
- informovať o kontaktnej osobe na riešenie bezpečnostných problémov a mechanizmoch na oznamovanie bezpečnostných incidentov.

Disciplinárny proces

Musí byť stanovený formálny disciplinárny proces pre zamestnancov, ktorí spôsobili porušenie informačnej bezpečnosti (pracovný poriadok, smernica o personálnej bezpečnosti a pod.).

Disciplinárny proces by sa nemal začať bez predošlého overenia, či naozaj došlo k narušeniu bezpečnosti vedomým konaním zo strany zamestnanca.

Formálny disciplinárny proces

Zabezpečenie korektného zaobchádzania so zamestnancami podozrivými z narušenia informačnej bezpečnosti ako aj vyvodenie adekvátnych opatrení v prípade jej narušenia.

Zabezpečenie primeranej reakcie na bezpečnostný incident berúc do úvahy faktory ako napr.:

- právne predpisy, vnútorné predpisy organizácie,
- závažnosť narušenia informačnej bezpečnosti,
- dopad na chod organizácie,
- či sa jedná o prvý alebo opakovaný priestupok,
- či bol narušiteľ primerane vyškolený,
- okamžité odňatie povinností, prístupových práv a privilégií vo výnimočných prípadoch zneužitia právomocí.

Disciplinárny proces slúži predovšetkým ako <u>odstrašujúci prostriedok:</u>

- vystríha zamestnancov pred porušovaním zákonov, riadiacich aktov a vnútorných predpisov organizácie, ako aj akýmkoľvek iným narušeniam bezpečnosti,
- demonštruje vážny záujem organizácie v oblasti dodržiavania zásad (nielen) informačnej bezpečnosti.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť ľudských zdrojov
ukončenie alebo zmena pracovného pomeru

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Cieľ

Zabezpečiť, aby zamestnanci opustili organizáciu alebo zmenili podmienky svojho pracovného vzťahu primeraným spôsobom, nenarúšajúcim informačnú bezpečnosť.

Definovanie zodpovedností - opustenie organizácie zamestnancom má byť riadené, bude navrátené všetko poskytnuté vybavenie, budú odňaté príslušné prístupové práva.

Zmena zodpovednosti a pracovného vzťahu v rámci organizácie by mala prebehnúť riadeným spôsobom (je potrebné mať definovaný postup a náležitosti takejto zmeny).

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vrátenie aktív

Pri ukončení pracovného vzťahu je zamestnanec povinný odovzdať všetky aktíva, ktoré sú v jeho správe a spolupracovať pri prevedení činností, ktoré vykonával, na iného zamestnanca.

Navrátanie aktív má byť evidované (výstupný list zamestnanca).

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vrátenie aktív

V procese výpovede musí byť zahrnuté odovzdanie:

- pracovných pomôcok,
- hardvérového a softvérového vybavenia,
- dokumentov v listinnej aj elektronickej forme, správy elektronickej pošty obsahujúce dôležité pracovné informácie,
- všetkých ostatných poznatkov dôležitých z hľadiska zaistenia kontinuity výkonu činností (nezdokumentované postupy, korešpondencia, špecifické znalosti nadobudnuté počas pracovného vzťahu...).

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vrátenie aktív – bezpečné vymazanie dát

Po odovzdaní zariadení ako napr. PC, prenosné disky, USB kľúče a iné prepisovateľné pamäťové zariadenia a médiá, ktoré boli používané zamestnancom a mohli by obsahovať citlivé dáta organizácie, musí byť vykonané bezpečné vymazanie týchto informácií. Až po jeho vykonaní je možné dané zariadenie alebo médium opätovne poskytnúť ďalšiemu používateľovi.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Odňatie prístupových oprávnení

Prístupové práva všetkých zamestnancov a zmluvných partnerov k informáciám a prostriedkom na ich spracúvanie musia byť na základe ukončenia pracovného resp. zmluvného vzťahu bezodkladne odobrané (cieľom je zabrániť neoprávnenému prístupu alebo zneužitiu prístupových práv).

KPMG
cutting through complexity™

Odňatie prístupových oprávnení

Prístupové práva, ktoré by mali byť odňaté alebo modifikované zahŕňajú:

- fyzický a logický prístup,
- kľúče, identifikačné karty,
- prostriedky na spracúvanie informácií,
- predplatené služby,
- odstránenie zo všetkej dokumentácie, ktorá ich zaraďuje k aktuálnym zamestnancom organizácie.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Záverečné zhrnutie

Najslabší článok „bezpečnostnej reťaze“ je

firewall

server

antivírus

databáza

NEZNALÝ ČLOVEK

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™