


TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ
Európsky fond regionálneho rozvoja

Riadiaci orgán pre OPIS

Sprostredkovateľský orgán pod
Riadiacim orgánom pre OPIS

Európska únia

Európsky fond regionálneho rozvoja
„Tvoríme vedomostnú spoločnosť“

Projekt je spolufinancovaný Európskou úniou

www.opis.sk
www.informatizácia.sk

Ministerstvo financií Slovenskej republiky

Národný projekt: Integrované obslužné miesta

BEZPEČNOSTNÁ POLITIKA PREVÁDZKARNE IOM

Názov obce:	
Sídlo:	
V zastúpení:	
Schválené dňa:	
Všeobecné záväzné nariadenie:	

Obsah

1. Úvod

Tento dokument upravuje riešenie bezpečnostnej politiky podľa požiadaviek výnosu MF SR č.55/2014 o štandardoch pre ISVS vo vzťahu k prevádzke pracoviska IOM.

1.1 Pojmy a skratky

V nasledujúcej tabuľke je uvedený popis skratiek používaných v rámci predkladaného dokumentu.

Skratka	Význam
IOM	Integrované obslužné miesto
IS	Informačný systém
ISVS	Informačný systém verejnej správy
MF SR	Ministerstvo financií SR
OÚ	Osobné údaje
SR	Slovenská republika
ÚPVS	Ústredný portál verejnej správy
ZEP	Zaručený elektronický podpis

2. Bezpečnostná politika prevádzkarne IOM

Pre potreby bezpečnostnej politiky v súlade s výnosom MF SR 55/2014 o štandardoch pre ISVS sa za povinnú osobu považuje prevádzkovateľ pracoviska IOM a za ISVS sa považuje IS IOM.

Členenie nasledovných kapitol zodpovedá oblastiam s potrebným riešením v rámci bezpečnostnej politiky podľa výnosu o štandardoch ISVS.

2.1 Bezpečnostné ciele povinnej osoby

Základné bezpečnostné ciele povinnej osoby pri prevádzke IS IOM sú v súlade s bezpečnostným projektom IS IOM podľa požiadaviek zákona 122/2013 v znení neskorších predpisov a vyhlášky Úradu na ochranu osobných údajov 164/2013 v znení neskorších predpisov:

- ochrana údajov a služieb pred zneužitím, falšovaním,
- zaistenie dôvernosti a integrity používateľských údajov,
- plynulá prevádzka v medziach predpísaných funkčných parametrov,
- prevádzka v súlade so všetkými relevantnými požiadavkami,
- ochrana dobrého mena prevádzkovateľa, SR, dodávateľa,
- dosiahnutie uvedených priorít efektívnym spôsobom.

Konkretizácia bezpečnostných cieľov je uvedená v Bezpečnostnom projekte IS IOM, časť Bezpečnostný zámer.

2.2 Spôsoby vyhodnocovania bezpečnostných cieľov

Za vyhodnocovanie bezpečnostných cieľov je zodpovedný zamestnanec povinnej osoby, ktorý je zodpovedný za informačnú bezpečnosť. Vyhodnocovanie bezpečnostných cieľov spočíva najmä vo vyhodnocovaní množstva, závažnosti a druhu bezpečnostných incidentov a úrovne implementácie bezpečnostných opatrení. Správu o dosahovaní bezpečnostných cieľov predkladá tento pracovník vedeniu povinnej osoby oficiálnou cestou minimálne raz ročne a vždy po zistení a vyšetrení bezpečnostného incidentu.

2.3 Úloha vedenia povinnej osoby pri zaisťovaní informačnej bezpečnosti

Vedenie povinnej osoby je zodpovedné za začlenenie tejto bezpečnostnej politiky do svojho systému riadenia informačnej bezpečnosti (napr. zosúladenie s bezpečnostnou politikou celej organizácie), jej rozpracovanie tam kde je to potrebné, realizáciu v nej uvedených aktivít. vrátane zodpovednosti za informovanie všetkých zamestnancov a tretích strán o obsahu bezpečnostnej politiky a povinnosti dodržiavať bezpečnostnú politiku.

Vedenie povinnej osoby zodpovedá za dodržiavanie informačnej bezpečnosti, dosahovanie cieľov informačnej bezpečnosti a zodpovedá za zabezpečenie potrebných zdrojov na dosahovanie cieľov informačnej bezpečnosti.
Vedenie povinnej osoby je zodpovedné za vysporiadanie sa s rizikami informačnej bezpečnosti a za formálnu akceptáciu zvyškových rizík.
Vedenie povinnej osoby zodpovedá za adekvátne vysporiadanie sa s bezpečnostnými incidentmi, vrátane komunikácie s dotknutými osobami, a vyvodenie dôsledkov.
Vedenie povinnej osoby poveruje zamestnancov výkonom bezpečnostných rolí a prideľuje adekvátne právomoci. Pri prideľovaní právomocí dbá najmä na požiadavky na nezlučiteľnosť rolí, kompetentnosť poverovaných pracovníkov plniť povinnosti vyplývajúce z rolí, povahu informačných aktív a riziká, ktoré majú na aktíva vplyv.

2.4 Všeobecné a špecifické zodpovednosti a povinnosti v oblasti informačnej bezpečnosti

Všetci zamestnanci povinnej osoby a tretie strany, ktoré prichádzajú do styku s informačnými aktívami povinnej osoby sú zodpovední za ochranu informačných aktív povinnej osoby. Sú povinní dodržiavať bezpečnostnú politiku, pravidlá informačnej bezpečnosti, oboznámiť sa s obsahom bezpečnostnej politiky a charakterom bezpečnostných opatrení. Nesmú obchádzať ani inak znižovať účinnosť bezpečnostných opatrení. O každom zistení porušenia bezpečnostnej politiky, bezpečnostnom incidente alebo snahe o obchádzanie bezpečnostných opatrení či znižovaní ich účinnosti sú povinní informovať pracovníka povereného informačnou bezpečnosťou a vedenie povinnej osoby.
Povinná osoba určí osobu zodpovednú za riadenie informačnej bezpečnosti pracoviska IOM, ktorá bude vykonávať činnosti minimálne v rozsahu uvedenom v tejto bezpečnostnej politike.

2.5 Povinnosť zaistenia nenarušenia informačnej bezpečnosti povinnej osoby

Povinná osoba je povinná implementovať a používať organizačné, personálne a technické opatrenia, ktorými zabezpečí zaistenie nenarušenia informačnej bezpečnosti. Rozsah potrebných opatrení je vymedzený Bezpečnostným projektom IS IOM, dokumentáciou IS IOM s prihliadnutím na špecifiká pracoviska IOM u povinnej osoby (analyzovaných v rámci vyhodnotenia rizík, viď. kap. 9).

2.6 Súlad bezpečnostnej politiky so všeobecne záväznými právnymi predpismi, vnútornými predpismi a zmluvnými záväzkami povinnej osoby

Bezpečnostná politika reflektuje požiadavky vyhlášky 55/2014 o štandardoch pre ISVS ako aj zákona 122/2013 a vyhlášky UOOU 164/2013 v znení neskorších predpisov v rozsahu primeranom IS IOM. Jej cieľom je predovšetkým stanoviť rámec pre ochranu informácií

uložených, spracovávaných a prenášaných v rámci IS IOM a to vrátane dokumentov v papierovej podobe a elektronickej podobe.

2.7 Požiadavky na IS IOM, spôsob vedenia a aktualizácie dokumentácie o IS IOM

Povinná osoba prevádzkuje IS IOM a udržiava o ňom dokumentáciu v súlade s prevádzkovým manuálom IS IOM v rozsahu a spôsobom v ňom stanoveným. Jedná sa predovšetkým o dokumentáciu rozsahu oprávnení pracovníkov IOM, administrátorov IOM, dokumentáciu všetkých servisných zásahov na technických prostriedkoch IOM, dokumentáciu o vykonaných pravidelných kontrolách a ich výsledkoch, dokumentáciu o podaniach uskutočnených prostredníctvom IS IOM v rozsahu a forme špecifikovaných prevádzkovým manuálom IS IOM, havarijných plánoch, plánoch obnovy a dokumentáciu nasadených bezpečnostných opatrení.

2.8 Rozsah a úroveň ochrany IS IOM vrátane hodnotenia slabých miest a ohrození

Hodnotenie slabých miest a ohrození je súčasťou bezpečnostnej dokumentácie podľa vyhlášky UOOU 164/2013. Povinná osoba pravidelne aktualizuje túto dokumentáciu v súlade s požiadavkami uvedenými v tejto dokumentácii, spravidla raz ročne alebo pri každej výraznej zmene prostredia, v ktorom je IOM prevádzkované. Povinná osoba na tento účel používa metodiku, ktorá je súčasťou prevádzkovej dokumentácie IS IOM. Rozsah ochrany IS IOM je daný technickým zabezpečením IOM, prevádzkarňou IOM, pracovníkmi IOM, komunikačnými kanálmi IS IOM a bezprostredným okolím IOM. Úroveň ochrany je daná požiadavkami na ochranu osobných údajov v rozsahu zákona 122/2013 v znení neskorších predpisov a to predovšetkým tak, aby sa zabezpečila dostupnosť, dôvernosť, integrita osobných údajov a dohľadateľnosť manipulácie a spracovania osobných údajov na všetkých použitých nosičoch vrátane papierových kópií, záložných médií, komunikačných kanáloch a všetkých elektronických dátových nosičoch.

2.9 Rámec pre manažment rizík v súvislosti s aktívami, od ktorých závisí činnosť IS IOM

Povinná osoba riadi riziká v súvislosti s prevádzkou IOM a IS IOM primárne v oblastiach, ktoré sú definované v záveroch bezpečnostného projektu tak, že implementuje v primeranej miere opatrenia spĺňajúce zásady bezpečnosti uvedené v záveroch bezpečnostného projektu. Povinná osoba vykonáva vyhodnotenie rizík informačnej bezpečnosti a návrh a implementáciu adekvátnych bezpečnostných opatrení na pokrytie rizík v prípade odlišnej klasifikácie rizík oproti predpokladanému štandardnému stavu pracoviska IOM podľa Bezpečnostnému projektu IS IOM.

2.10 Rozsah a periodicita auditu bezpečnosti IS IOM, určenie udalostí v IS IOM, o ktorých sa vytvára záznam auditu

Rozsah a periodicita auditu bezpečnosti IS IOM sú stanovené v prevádzkovom manuáli IS IOM. Udalosti, o ktorých sa vykonáva automatický záznam auditu, sú definované v prevádzkovom manuáli IS IOM. Samostatne sa vykonávajú záznamy o všetkých udalostiach, ktoré môžu mať vplyv na bezpečnosť informácií IS IOM či už v elektronickej alebo papierovej podobe, na všetkých typoch nosičov. Jedná sa najmä o pokus o neoprávnené použitie IS IOM, pokus o zneužitie IS IOM, vírusová infekcia, neoprávnený pokus o získanie prístupových práv k IS IOM, pokus o narušenie bezpečnostných opatrení, vrátane opatrení fyzickej bezpečnosti, pokus o odvodenie informácií o podaniach na základe pozorovania pracoviska IOM, pokus o inštaláciu neautorizovaných záznamových systémov (kamery, mikrofóny).
Záznamy auditu sa vykonávajú aj v rámci auditu informačnej bezpečnosti podľa použitej metodiky auditu.

2.11 Smernica pre zálohovanie, určenie skupín údajov a periodicity ich zálohovania

Všetky informácie v elektronickej forme, potrebné pre prevádzkovanie IS IOM, sú zálohované na centrálnej infraštruktúre prevádzkovateľa IS IOM. Zálohovanie sa na prevádzkarňach IOM nevykonáva. Dokumentácia v papierovej forme podlieha režimu stanovenému registratúrnym poriadkom prevádzkovateľa IOM.

2.12 Periodicita monitorovania bezpečnosti a aktualizácia softvéru

Povinná osoba musí udržiavať programové vybavenie technických prostriedkov IOM v aktuálnom stave tak, aby sa minimalizovala možnosť zneužitia softvérových zraniteľností na narušenie bezpečnosti IS IOM a IOM. Aktualizácia sa musí vykonávať priebežne.
V prípade, že to nie je možné, je potrebné zabezpečiť pravidelnú aktualizáciu podľa zásad uvedených v záveroch bezpečnostného projektu. Povinná osoba musí udržiavať aktuálny predovšetkým systém na ochranu proti počítačovým vírusom a škodlivému kódu, operačný systém počítačov IOM, aplikačný softvér IS IOM, ostatný aplikačný softvér používaný na pracovisku IOM, operačný systém alebo firmvér všetkých komunikačných prostriedkov, ktoré sa využívajú pri poskytovaní služieb IOM (napríklad internetové smerovače, firewally, sieťové prvky).

2.13 Zoznam dokumentov potrebných na zaistenie informačnej bezpečnosti

Dokumentácia potrebná na zaistenie informačnej bezpečnosti je vytváraná v rozsahu požiadaviek vyhlášky 55/2014 o štandardoch pre ISVS a vyhlášky UOOU 164/2013 znení neskorších predpisov. Jedná sa predovšetkým o bezpečnostný projekt IS IOM -

bezpečnostný zámer IS IOM, analýzu bezpečnosti IS IOM a závery bezpečnostného projektu – zásady bezpečnosti IS IOM, bezpečnostnú politiku IS IOM.

2.14 Postup a periodicita revízie bezpečnostnej politiky povinnej osoby

Bezpečnostná politika musí byť revidovaná v súlade s bezpečnostnou dokumentáciou a prevádzkovým manuálom IS IOM minimálne raz ročne a pri akejkoľvek zmene prostredia či významnej udalosti, ktorá môže mať vplyv na informačnú bezpečnosť IS IOM

2.15 Organizačné zabezpečenie realizácie a dodržiavania bezpečnostnej politiky IS IOM

Povinná osoba písomne ustanoví zodpovedného zamestnanca zodpovedného za dodržiavanie bezpečnostnej politiky IS IOM a vykoná o tom zápis, ktorý sa stáva prílohou tejto bezpečnostnej politiky.

2.16 Určenie konkrétnej zodpovednosti za jednotlivé aktíva povinnej osoby

Povinná osoba písomne ustanoví zodpovedných zamestnancov zodpovedných za jednotlivé aktíva IS IOM a vykoná o tom zápis, ktorý sa stáva prílohou tejto bezpečnostnej politiky.

2.17 Určenie privilegovaných používateľských rolí, určenie bezpečnostných požiadaviek na jednotlivé roly, určenie požiadaviek na nezlučiteľnosť rolí.

Pri prideľovaní privilegovaných používateľských rolí dbá povinná osoba na požiadavky na nezlučiteľnosti rolí. Medzi navzájom nezlučiteľné role patria najmä: správca systému, operátor, používateľ IS IOM (pracovník IOM), audítor a programátor.