Politika informačnej bezpečnosti

(skrátená verzia)

december 2011

1. Úvod

Politika informačnej bezpečnosti (ďalej len „politika“) je spracovaná v súlade s:

a) § 28 výnosu MF SR č. 312/2010 Z. z. zo dňa 09. júna 2010 o štandardoch pre informačné systémy verejnej správy (ďalej len „výnos MF SR“),
b) kap 4.3.1 medzinárodnej normy ISO/IEC 27001:2005,
c) kap 5. medzinárodnej normy ISO/IEC 27002:2005.

Politika určuje hlavné ciele, zásady a princípy systému riadenia informačnej bezpečnosti budovaného a využívaného so snahou minimalizovať možnosti úniku a zneužitia citlivých informácií vyskytujúcich sa pri činnosti Ministerstva dopravy, výstavby a regionálneho rozvoja Slovenskej republiky (ďalej len „ministerstvo“).

2. Základné údaje a pôsobnosť ministerstva

Podľa zákona č. 575/2001 Z. z. o organizácii vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov je ministerstvo ústredným orgánom štátnej správy.

Pôsobnosť ministerstva je definovaná v štatúte ministerstva a podrobnejšie v organizačnom poriadku ministerstva. Dokumenty sú vystavené na webovom sídle ministerstva v záložke „Ministerstvo“.

3. Rozsah pôsobnosti systému riadenia informačnej bezpečnosti

Systém riadenia informačnej bezpečnosti je vybudovaný v súlade s požiadavkami výnosu MF SR a medzinárodnej normy ISO/IEC 27001:2005.

Systém riadenia informačnej bezpečnosti ministerstva sa uplatňuje:

a) pri všetkých činnostiach ministerstva v rámci organizačných útvarov podľa platnej organizačnej štruktúry,
b) na všetky prevádzkované informačné systémy a siete po hraničné zariadenia pre komunikáciu s externým prostredím.

Systém riadenia informačnej bezpečnosti ministerstva sa nevzťahuje na agendu utajovaných skutočností.

4. Ciele systému riadenia informačnej bezpečnosti a ich vyhodnocovanie

Ciele systému riadenia informačnej bezpečnosti ministerstva sú v rámci tejto politiky rozdelené na:

a) globálne ciele systému riadenia informačnej bezpečnosti,
b) hlavné ciele systému riadenia informačnej bezpečnosti,
c) operatívne ciele systému riadenia informačnej bezpečnosti.

4.1 Globálne ciele systému riadenia informačnej bezpečnosti ministerstva

Globálnymi cieľmi sú:

a) plniť požiadavky v oblasti systému riadenia informačnej bezpečnosti určené výnosom MF SR,
b) budovať systém riadenia informačnej bezpečnosti existujúci na ministerstve tak, aby splnil všetky požiadavky výnosu MF SR a medzinárodnej normy ISO/IEC 27001,
c) zabezpečiť integritu, dostupnosť a dôvernosť informácií.

4.2 Hlavné ciele systému riadenia informačnej bezpečnosti

Hlavné ciele systému riadenia informačnej bezpečnosti budovaného a využívaného na ministerstve sú:

a) poskytovať usmernenie pre riadenie a podporu informačnej bezpečnosti v súlade s platnými predpismi SR a EÚ,
b) riadiť informačnú bezpečnosť z pohľadu ministerstva,
c) navrhovať bezpečnostné riešenia na základe kvalifikovanej analýzy rizík, bezpečnostnými riešeniami udržiavať informačnú bezpečnosť na požadovanej úrovni,
d) dosahovať primeranú ochranu kľúčových systémov a ich aktív,
e) zabezpečiť školenia zamestnancov ministerstva, zmluvných strán a tzv. tretích strán tak, aby rozumeli svojim zodpovednostiam, ktoré sa týkajú systému riadenia informačnej bezpečnosti a svoju činnosť vykonávali v súlade s bezpečnostnými zámermi ministerstva,
f) zabrániť neautorizovanému vniknutiu do priestorov ministerstva s cieľom zničenia, poškodenia, ohrozenia priestorov alebo aktív,
g) zabezpečiť riadenie logického prístupu k spracúvaným a spravovaným informáciám s uplatnením princípu „need to know“ (odporučaná interpretácia: „prístup len k tomu, čo potrebuješ“),
h) zabezpečiť správnu a bezpečnú prevádzku prostriedkov spracúvajúcich informácie,
i) zabrániť prerušeniam v činnosti útvarov ministerstva. Chrániť všetky informačné systémy a siete ministerstva tak, aby nedošlo k ohrozeniu kontinuity činnosti ministerstva z dôvodu havárie alebo výpadku informačných systémov. Zabezpečiť obnovu činnosti havarovaných systémov bez finančných strát a straty dobrého mena,
j) monitorovať prostredie, evidovať a ošetrovať podozrivé udalosti a bezpečnostné incidenty tak, aby sa predchádzalo ich opakovanému výskytu,
k) vyhnúť sa porušeniam zákonných, regulačných a zmluvných bezpečnostných požiadaviek.

4.3 Operatívne ciele systému riadenia informačnej bezpečnosti

Operatívne ciele sú určené „Plánom ošetrenia rizík“. Operatívne ciele súvisia s realizáciou jednotlivých projektov v rámci dobudovávania a zlepšovania systému riadenia informačnej bezpečnosti.

5. Podpora systému riadenia informačnej bezpečnosti zo strany vedúcich štátnych zamestnancov a vedúcich zamestnancov ministerstva (ďalej len „vedúci zamestnanci“)

Vedúci zamestnanci ministerstva aktívne podporujú zavedenie systému riadenia informačnej bezpečnosti, a to:

a) **zadávaním jasných pokynov** týkajúcich sa všetkých aspektov informačnej bezpečnosti,
b) **preukázaním angažovanosti** prostredníctvom prerokovania všetkých dokumentov súvisiacich s riadením informačnej bezpečnosti a poskytovaním zdrojov potrebných na jej praktické zabezpečovanie, ako súčasť procesného riadenia,
c) **prideľovaním bezpečnostných zodpovedností** v rámci systému riadenia informačnej bezpečnosti.

6. Bezpečnostná klasifikácia korešpondencie a slobodný prístup k informáciám

Ministerstvo má v súlade s bezpečnostnou politikou a vnútornou smernicou, ktorá definuje pravidlá klasifikácie informácií, ich inventarizáciu a manipuláciu s nimi schválený katalóg informačných aktív, v ktorom musí byť aktívum klasifikované jedným z nasledovných stupňov dôvernosti:

a) verejné,
b) interné,
c) chránené.

Adresát písomnej korešpondencie obsahujúcej stupeň dôvernosti, musí s touto informáciou primerane nakladať.

Ministerstvo je povinné poskytovať informácie podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

7. Elektronická pošta

Ministerstvo má nastavené bezpečnostné pravidlá pre komunikáciu elektronickej pošty. Súčasťou elektronickej pošty je usmernenie s textáciou „Táto správa a všetky k nej priložené súbory sú citlivé z hľadiska stupňa dôvernosti a sú určené výhradne adresátovi (-tom) správy. Obsah správy a jej príloh môže podliehať ochrane podľa osobitných predpisov. Pokiaľ nie ste oprávneným adresátom tejto správy, prosím, nešírte túto správu, nezverejňujte, nekopírujte a ani inak s touto správou a jej prílohami nezaobchádzajte. V prípade, že ste túto správu dostali neoprávnene, prosím, upovedomte okamžite jej odosielateľa, že Vám táto správa bola doručená a vymažte ju zo svojho počítačového systému“.

Adresát, ktorému bola elektronická pošta doručená neoprávnene, je povinný postupovať podľa tejto správy.

8. Prehlásenie o aplikovateľnosti systému riadenia informačnej bezpečnosti ministerstva

Prehlásenie o aplikovateľnosti systému riadenia informačnej bezpečnosti ministerstva je povinnou dokumentáciou vyplývajúcou z medzinárodnej normy ISO/IEC 27001:2005, ak organizácia požaduje certifikáciu systému riadenia informačnej bezpečnosti podľa tejto medzinárodnej normy.

Ministerstvo má schválený dokument „**Prehlásenie o aplikovateľnosti, verzia 1,02 zo dňa 08. 04. 2010**“.

Prehlásenie o aplikovateľnosti systému riadenia informačnej bezpečnosti uvádza ciele riadenia a opatrenia, ktoré boli vybrané pre systém riadenia informačnej bezpečnosti ministerstva.

Výber cieľov a opatrení je prepojený s výsledkami procesu ohodnocovania a ošetrovania rizík dokladovaného správami z opakovanej analýzy rizík.

9. Medzinárodný certifikát systému manažérstva podľa ISO/IEC 27001:2005

Ministerstvo získalo v mesiaci **máj 2010 medzinárodný certifikát pre systém manažérstva podľa ISO/IEC 27001:2005**.

V roku 2011 ministerstvo obhájilo medzinárodný certifikát v rámci kontrolného medzinárodného auditu.

Ján Figeľ, v.r.
1. podpredseda vlády a minister dopravy,
výstavy a regionálneho rozvoja
Slovenskej republiky

Medzinárodný certifikát systému riadenia informačnej bezpečnosti ministerstva

CERTIFIKÁT

pre systém manažérstva podľa
ISO/IEC 27001:2005

Podľa postupov TÜV NORD CERT sa týmto potvrdzuje, že

Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky
Námestie slobody 6
810 05 Bratislava
Slovenská republika

s miestami Nám. 1. mája, 810 05, Bratislava 15 a Lamačská cesta, 810 05, Bratislava 15, Slovak Republic

používa systém manažérstva v súlade s horeuvedenou normou
pre oblasť platnosti

Ochrana informácií pri všeobecnej správe a pri hlavných činnostiach ministerstva vykonávaných v súlade so slovenskými zákonmi a regulačnými opatreniami.

Prehlásenie o aplikovateľnosti, Verzia 1.02 z 08.04.2010

Registračné číslo certifikátu 44 121 100615 Platný do 2013-05-18
Správa z auditu č. 3508 6086

Certifikačné miesto Essen, 2011-09-09
pri TÜV NORD CERT GmbH

Táto certifikácia bola vykonaná podľa predpisov TÜV NORD CERT pre auditovanie a certifikáciu a podlieha pravidelným kontrolným auditom.

TÜV NORD CERT GmbH Langemarckstrasse 20 45141 Essen www.tuev-nord-cert.de

Deutscher Akkreditierungs Rat
TGA-ZM-07-06-20