[redacted]

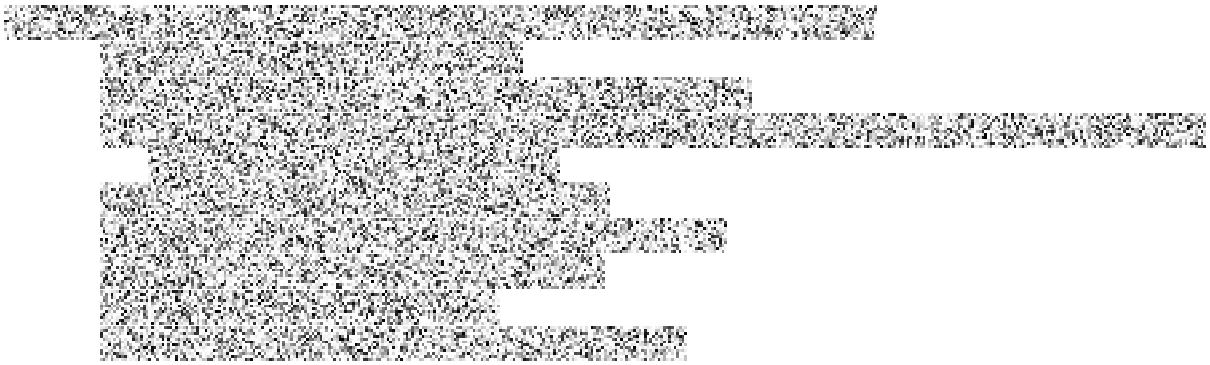
[redacted]	
Následný audit – termín:	-

Dátum: 20.09.2015

Ing. Branislav Chmel

Vedúci audítor

Podpis



- konzultácie a výpočtové práce pomocou konečných prvkov podľa objednávky
- organizácia stretnutí s tvorcami programových súborov, stretnutia užívateľov

1.2. Prehlásenie o aplikovateľnosti

Prehlásenie o aplikovateľnosti schválené dňa 20.08.2014 vedením organizácie uvádza vylúčené opatrenia:

- ☐ žiadne
- ☒ A.10.1.1 Politika pri používaní opatrení na šifrovanie
- ☒ A.10.1.2 Riadenie šifrovacích kľúčov
- ☒ A.14.1.2 Zabezpečenie aplikačných služieb vo verejných sieťach
- ☒ A.14.1.3 Ochrana pri transakciách aplikačných služieb
- ☒ A.18.1.5 Nariadenie o kryptografických opatreniach

Predložené Prehlásenie o aplikovateľnosti uvádza ďalšie opatrenia, nad rámec prílohy A normy STN ISO/IEC 27001:2014: -

2.stupeň certifikačného auditu bol vo vyššie uvedenej organizácii vykonaný audítormi certifikačného orgánu TÜV SÜD Slovakia s.r.o. na základe normy **STN ISO/IEC 27001:2014**. Ďalším podkladom pre audit bola príručka ISMS PK.01.100 vyd.1 rev.2 z 30.06.2015 organizácie a jednotlivé dokumentované postupy citované v tejto príručke, rovnako ako ďalšia dokumentácia, ktorá bola k dispozícii na jednotlivých úsekoch podľa organizačnej schémy. Organizácia bola už v predchádzajúcom období certifikovaná v systéme manažérstva kvality podľa ISO 9001 a v systéme environmentálneho manažérstva podľa ISO 14001 certifikačným orgánom TÜV SÜD Slovakia s.r.o.

Správa je členená podľa štandardného spôsobu používaného certifikačným orgánom TÜV SÜD Slovakia s.r.o.

Doplňujúce poznámky: žiadne

[redacted]

K predchádzajucemu auditu neboli identifikované nezhody.

4. Vykonanie auditu

4.1 Auditované požiadavky a postup

Organizácia **TEN SLOVAKIA, s.r.o.** disponuje systémom riadenia informačnej bezpečnosti, ktorý spĺňa požiadavky normy **STN ISO/IEC 27001:2014**.
Pri audite bolo zistené, že rozsah a hranice ISMS zohľadňujú charakteristiku organizácie, aktív a technológií. Prehlásenie o aplikovateľnosti odráža činnosti a definuje hranice na základe analýzy rizík. Stanovené vylúčenia a výbery opatrení boli audítormi akceptované vzhľadom k rozsahu ISMS organizácie. Sú vytvorené predpoklady pre ďalšie zlepšovanie systému riadenia informačnej bezpečnosti. Systém riadenia informačnej bezpečnosti je založený na aplikácii a používaní dokumentovaných postupov, monitorovaní efektívnosti uplatňovaných opatrení s cieľom zlepšovať procesy systému.

Pravidelne sa konajú porady vedenia, na ktorých sa vykonáva preskúmanie systému riadenia informačnej bezpečnosti a nápravných opatrení k výsledkom interných auditov a k plneniu stanovených cieľov. Vedenie organizácie poskytuje potrebné zdroje (finančné a organizačné) k zaisteniu účinnosti systému manažérstva.

V priebehu auditu sa audítori mohli presvedčiť o kvalifikácii a odborných skúsenostiach preverovaných zamestnancov. Organizačná štruktúra a zodpovednosti zamestnancov sú stanovené a sledovateľné.

Ďalej boli vyhodnotené nasledujúce skutočnosti:
- ✓ účinnosť ISMS so zreteľom na realizáciu politiky integrovaného manažérskeho systému
- ✓ riadenia rizika - procesy posúdenia a ošetrenia rizika (postup pre identifikáciu aktív, hrozieb, hodnotenie rizík, stanovenie opatrení a cieľov ISMS),
- ✓ zdroje, úlohy, zodpovednosti, povinnosti a právomoci,
- ✓ odborná spôsobilosť, príprava a povedomie,
- ✓ komunikácia, účasť a konzultácie,
- ✓ dokumentácia, riadenie dokumentov,

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Používanie certifikátu a značky TÜV SÜD Slovakia

Certifikát a značka sú používané povoleným spôsobom, t.j. v súlade s pravidlami CO SM TÜV SÜD Slovakia s.r.o. a bez väzby na výrobky.

[redacted] prípade

- ☑ vedúci auditu odporúča ďalšie trvanie platnosti certifikátu
- ❑ vedúci auditu neodporúča ďalšie trvanie platnosti certifikátu
- ☑ budúci audit je plánovaný podľa programu auditu ako dozorný v období október 2016 pri ktorom musia byť preverené povinné prvky 4, 5, 6, 7, 8, 9, 10 normy a A.5 - A.18 prílohy A normy. Ďalšie preverované prvky normy budú stanovené vedúcim audítorom v pláne auditu.

Certifikačné miesto musí byť informované o všetkých významných zmenách vo vzťahu k systému manažmentu bezpečnosti informácií.

Doplňujúce poznámky:

stanovenie
resp.
-3/+0
recertifikačného
termín

nápravných