Zmluva o dielo
uzavretá podľa § 536 a násl. Obchodného zákonníka na realizáciu „Audit bezpečnosti IS – Ochrana osobných údajov",

č. EMM: Z 0053/2010

ČLÁNOK I
Zmluvné strany

Objednávateľ:

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky
Štefanovičova 3,
810 05 Bratislava 15

Zastúpený:	Ing. Lucia Gocníková, predsedníčka úradu
Bankové spojenie:	Štátna pokladnica č.ú.: 7000068787/8180
IČO:	30810710

a

Zhotoviteľ:

EMM spol. s r. o.
Sekurisova 16
841 02 Bratislava

Zastúpený:	Mária Schill, konateľka
Zmocnenec pre:	
a) zmluvné rokovanie	Mária Schill, konateľka
b) technické rokovanie	Peter Belák, vedúci projektu
Bankové spojenie:	ČSOB Bratislava č.ú.: 0584749903/7500
IČO:	17316260
IČDPH:	SK2020316529

Zapísaný v Obchodnom registri Okresného súdu Bratislava I, oddiel S.r.o., vložka číslo: 686/B

ČLÁNOK II

Východiskové podklady

1. Východiskovým podkladom na uzavretie tejto zmluvy o dielo na realizáciu „Audit bezpečnosti informačného systému – Ochrana osobných údajov" je ponuka zhotoviteľa zo dňa 17.12.2010 (v Prílohe č. 1).

ČLÁNOK III

Predmet zmluvy

1. Predmetom zmluvy je záväzok zhotoviteľa zrealizovať dielo „Audit bezpečnosti informačného systému – Ochrana osobných údajov". Detailná špecifikácia diela je uvedená v Prílohe č. 1 – Ponuka zhotoviteľa.

ČLÁNOK IV

Cena predmetu zmluvy

1. Cena predmetu zmluvy je určená podľa § 3 zákona Národnej rady Slovenskej republiky č. 18/1996 Z. z. o cenách vo výške 35 628,60 EUR (slovom tridsaťpäťtisíc šesťstodvadsaťosem Eur šesťdesiat centov) vrátane DPH 19%, z toho

   základ pre DPH: 29 940,00 EUR
   DPH 19 %: 5 688,60 EUR

2. Zhotoviteľovi vznikne právo fakturovať zrealizované dielo na základe preberacieho protokolu podpísaného zodpovedným pracovníkom objednávateľa.
3. Splatnosť faktúry je 14 dní od jej doručenia objednávateľovi.
4. Kalkulácia ceny predmetu zmluvy je v Prílohe č. 1 k tejto zmluve.
5. Ak v dôsledku administratívneho zásahu štátu dôjde v čase plnenia tejto zmluvy k zmene DPH, alebo iným opatreniam, ktoré budú mať vplyv na cenu predmetu zmluvy, zhotoviteľ je povinný upraviť primerane cenu predmetu zmluvy, ak sa naň tieto opatrenia budú vzťahovať.

ČLÁNOK V

Doba trvania zmluvy

1. Zmluva sa uzatvára na dobu určitú, podľa harmonogramu plnenia predmetu zmluvy uvedeného v Prílohe č. 1 k tejto zmluve.

ČLÁNOK VI

Miesto plnenia zmluvy

1. Miestom plnenia zmluvy je sú pracoviská a priestory objednávateľa a zhotoviteľa.

ČLÁNOK VII

Ochrana informácií

1. Zhotoviteľ vyhlasuje, že bol oboznámený s tým, že objednávateľ prevádzkuje informačný systém, ktorý podlieha režimu ochrany podľa zákona Národnej rady Slovenskej republiky č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.
2. Zhotoviteľ sa zaväzuje:
   a) uchovávať mlčanlivosť o všetkých skutočnostiach, (citlivé údaje, ktorými sú napr. dokumenty o objednávateľovi, jeho klientoch, obchodných partneroch, obchodoch, osobné údaje podľa zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov), o ktorých sa dozvedel v súvislosti s plnením tejto zmluvy, a neposkytnúť ich tretej osobe,
   b) že jeho zamestnanci, ktorí budú osobne zabezpečovať predmet plnenia podľa tejto zmluvy, zachovajú mlčanlivosť o všetkých skutočnostiach, o ktorých sa oboznámia pri plnení tejto zmluvy po dobu plnenia tejto zmluvy aj po jeho splnení,
3. S citlivými údajmi objednávateľa sa môžu oboznamovať len určené osoby, ktoré spĺňajú stanovené predpoklady a ktoré písomne určil objednávateľ na styk s citlivými údajmi. Určené osoby zhotoviteľ poučí o príslušných predpisoch o ochrane údajov a z nich vyplývajúcich povinnostiach v zmysle § 17 zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov. Určené osoby, ktoré boli poučené o povinnostiach pri spracúvaní citlivých údajov sú povinné zabezpečiť, aby sa o citlivých údajoch nedozvedela nepovolaná osoba alebo neboli inak zneužité.
4. Utajenie sa netýka informácií, technológií a techník všeobecne známych, informácií, ktoré boli preukázateľne nezávisle vypracované alebo s nimi druhá zmluvná strana vyslovila písomný súhlas.

ČLÁNOK VIII

Osobitné ustanovenia

1. Zmluvné strany sa dohodli, že za podstatné porušenie povinností sa považuje najmä:
   a) nedodanie predmetu zmluvy v rozsahu prác uvedeného v Prílohe č. 1 k tejto zmluve,
   b) nevymenovanie zodpovedného pracovníka objednávateľa a vedúceho projektu zhotoviteľa,
   c) nesplnenie povinností objednávateľa špecifikovaných v Prílohe č. 1 k tejto zmluve,
   d) nedodržanie termínu plnenia zmluvy podľa harmonogramu plnenia predmetu zmluvy, ktorý je uvedený v Prílohe č. 1 k tejto zmluve,
   e) vada plnenia.
2. Zmluvné strany sa dohodli, že za podstatné porušenie zmluvných povinností s možnosťou odstúpenia od zmluvy a vymáhania náhrady škody týmto spôsobenej, budú považovať aj porušenie zachovania mlčanlivosti.
3. Zmluvné strany sa zaväzujú, že vzniknuté problémy budú operatívne riešiť na úrovni zodpovedného pracovníka objednávateľa a vedúceho projektu zhotoviteľa.

ČLÁNOK IX

Zmluvná pokuta a náhrada škody

1. V prípade nedodržania termínu realizácie diela podľa Prílohy č. 1 je objednávateľ oprávnený požadovať od zhotoviteľa zaplatenie zmluvnej pokuty vo výške 0,05% za každý aj začatý deň meškania.

2. V prípade nedodržania splatnosti správne vystavenej faktúry za realizáciu diela podľa Prílohy č. 1 je zhotoviteľ oprávnený požadovať od objednávateľa zaplatenie úroku z omeškania vo výške 0,05% za každý aj začatý deň meškania.
3. V prípade oprávneného odstúpenia od zmluvy, je strana, ktorá odstupuje oprávnená požadovať od protistrany pokutu vo výške 10% z ceny predmetu zmluvy.
4. Zmluvné strany sa dohodli, že objednávateľ aj zhotoviteľ sú oprávnení domáhať sa náhrady škody spôsobenej druhou zmluvnou stranou.
5. Vzájomné pohľadávky vzniknuté porušením zmluvných povinností podľa tejto zmluvy bude možné započítať v súlade s § 364 Obchodného zákonníka.

ČLÁNOK X
Záruky

1. Zhotoviteľ poskytuje na dielo záruku v trvaní 12 mesiacov odo dňa podpisu preberacieho protokolu, mimo platných legislatívnych zmien.
2. Zhotoviteľ sa zaväzuje, že bezplatne odstráni vady predmetu zmluvy v súlade s podmienkami uvedenými v Prílohe č. 1 k tejto zmluve.

ČLÁNOK XI
Záverečné ustanovenia

1. Zmluva nadobúda platnosť a účinnosť dňom jej podpisu oboma zmluvnými stranami.
2. Táto zmluva sa môže meniť po vzájomnej dohode oboch zmluvných strán formou písomného číslovaného dodatku, podpísaného štatutárnymi zástupcami zmluvných strán.
3. Zmluvné vzťahy, ktoré neupravuje táto zmluva sa riadia príslušnými ustanoveniami Obchodného zákonníka a príslušnými všeobecne záväznými právnymi predpismi.
4. Neoddeliteľnou súčasťou tejto zmluvy je Prílohy č.1 – ponuka zhotoviteľa
5. Zmluva je vyhotovená v štyroch rovnopisoch, po dva rovnopisy pre každú zmluvnú stranu.

V Bratislave, dňa 22.12.2010

Za objednávateľa:

.....
Ing. Lucia Gocníková
predsedníčka úradu

V Bratislave, dňa.....

Za zhotoviteľa:

.....
Mária Schill
konateľka EMM, spol. s r.o.

PRÍLOHA Č. 1 – PONUKA ZHOTOVITEĽA

Audit bezpečnosti IS – OOÚ

Tento dokument obsahuje citlivé informácie.

Záujemca:	EMM, spol. s r.o. Sekurisova 16 841 02 Bratislava
Obstarávateľ:	Úrad normalizácie, metrológie a skúšobníctva SR Štefanovičova 3 810 05 Bratislava
Miesto a dátum tlače:	Bratislava, 17.12.2010

Dokument

Ponuka:	Audit bezpečnosti IS – OOÚ
Dátum:	17.12.2010
Projektový manažér:	Peter Belák

Schválené

Meno	Funkcia
František Boda	riaditeľ úseku BIS

Rozdeľovník

Kópia číslo	Distribúcia
1	ÚNMS SR

Spolupracovali na dokumente

Meno	Funkcia
Milan Ďorda	senior manager
Peter Belák	analytik

Obsah

1. Úvod

Systém riadenia a efektívne zabezpečovanie činností spoločnosti sú závislé od nepret
funkčnosti informačného systému, ako aj údajov v ňom spracovávaných a poskytova
zamestnancom a riadiacim pracovníkom jednotlivých organizačných jednotiek spoločnos

Údaje sú práve tým najdôležitejším aktívom pre spoločnosť. Ich prípadné poškod
modifikácia alebo strata môže mať vážne dôsledky. Samotná dôležitosť niektorých t
údajov je daná aj osobitnou pozornosťou v legislatíve SR.

Audit bezpečnosti informačného systému sa vyžaduje v špecifických prípadoch legislat
Samotné overenie súladu bezpečnosti informačného systému je aj v záujme organi
či sú dodržané všetky potrebné opatrenia stanovené národnými alebo medzinárod
normami a štandardmi. Audit bezpečnosti IS zameraný na ochranu osobných údaj
čiastkovou úlohou komplexného auditu bezpečnosti.

2. Charakteristika ponuky

2.1 Audit všeobecne

Audit je proces komplexného posúdenia, či skutočný stav definovaného systému zodpovedá predpokladanému, predpísanému alebo deklarovanému stavu. Predmetom auditu je aj hodnotenie efektívnosti a úplnosti postupov. Audit navrhuje zmeny k lepšiemu, orientuje sa na obmedzenie podnikateľských rizík a podáva o týchto skutočnostiach správu.

Audit bezpečnosti informačného systému predstavuje posúdenie návrhu riešenia, prevádzky, prípadne inovácie celého informačného systému z hľadiska ochrany a schopnosti plniť povinnosti ukladané zákonnými normami a vnútornými predpismi a požiadavkami organizácie. Audit bezpečnosti IS teda vychádza z predpokladaného alebo požadovaného stavu bezpečnosti IS, ktorý poskytuje schválená bezpečnostná politika, analýza rizík, bezpečnostná dokumentácia alebo závery predchádzajúceho auditu.

Audit bezpečnosti IS posudzuje úroveň kontrolných prvkov na úrovni aplikácií informačného systému a hodnotí kvalitu riadenia relevantných aspektov IS. Audit posudzuje prvky regulujúce prístup k aplikáciám a údajom v nich spracovávaných, prvky pre kontrolu vstupných dát a pre verifikáciu vstupných dát, pre zabezpečenie správnosti prenosu a spracovania údajov. Hodnotená je úroveň manažmentu IS z hľadiska jeho plánovacej, organizačnej, personálnej, riadiacej a kontrolnej funkcie vo vzťahu k bezpečnosti IS. Posudzovaný je systém riadenia vývoja IS a riadenia samotnej prevádzky IS. Hodnotený je celkový stav a úroveň ochrany organizácie, bezpečnosť IS ako celku i jeho jednotlivých častí a realizácia opatrení a protiopatrení na minimalizáciu alebo elimináciu existujúcich rizík.

Audit bezpečnosti IS je činnosť získavania a vyhodnocovania poznatkov o bezpečnosti informačného systému a o údajoch v ňom obsiahnutých, s cieľom:

- zistiť mieru súladu medzi bezpečnostnou politikou a skutočnou situáciou,
- poskytnúť primeranú istotu o tom, že bezpečnosť IS je na požadovanej úrovni, a že bezpečnostný systém organizácie neobsahuje významné medzery,
- oznámiť zistené výsledky, prípadne navrhnúť možné riešenia zistených nedostatkov.

Pri audite je možné sa využiť metodiku COBIT (Control Objectives for Information and related Technology), ktorá tvoria rámec pre realizovanie auditu v oblasti informačných systémov. COBIT v základných doménach (plánovanie a organizácia, obstarávanie a implementácia, dodávky a podpora, monitoring) definuje procesy prebiehajúce v IS.

V rámci týchto procesov sú definované ciele, ktoré má spĺňať bezpečný IS. Definované ciele nie sú konečné a jediné, organizácia si podľa vlastných potrieb môže doplniť ďalšie.

2.2 Aplikované normy, postupy a metodiky

Počas auditu budú použité normy, postupy a metodiky v súlade s najnovšími poznatkami z oblasti bezpečnosti. Pri realizácii jednotlivých činností auditu je možné použiť nasledovné normy, postupy a metodiky:

Oblasť auditu	metodické postupy ISACA, COBIT
Oblasť manažmentu rizík a návrhu bezpečnostných opatrení	ISO 13335, ISO 27000, ITSEC, VdS
Oblasť správy bezpečnosti	ISO 13335
Oblasť technickej bezpečnosti	VdS, relevantné STN
Oblasť ochrany údajov	zákon 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov

Postupy použité pri audite budú vychádzať z:

1. Požiadaviek slovenskej legislatívy kladených na ochranu osobných údajov, zákon č. 428/2002 Z. z. v znení neskorších predpisov.
2. Požiadaviek medzinárodných štandardov určených pre bezpečnosť informačných systémov, fyzickú a personálnu bezpečnosť, bezpečnosť telekomunikačnej prevádzky.
3. Medzinárodných noriem pre oblasť auditu bezpečnosti informačných systémov.

3. AUDIT BEZPEČNOSTI IS - OOÚ

Dôvodom realizácie auditu bezpečnosti IS – OOÚ na Úrade pre normalizáciu, metrológiu a skúšobníctvo SR je uspokojenie požiadavky objednávateľa s uplatnením opatrení vyplývajúcich zo zákona číslo 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

3.1 Audit bezpečnosti IS - OOÚ

Na základe požiadavky obstarávateľa bude vykonaný audit bezpečnosti IS zameraný na posúdenie spoľahlivosti a bezpečnosti informačného systému z hľadiska zabezpečenia dôvernosti, integrity a dostupnosti spracúvaných osobných údajov.

Audit bude obsahovať posúdenie IS na základe bezpečnostného projektu a príslušných technických, organizačných a personálnych opatrení, ktoré bezpečnostný projekt vymedzuje na eliminovanie hrozieb a rizík pôsobiacich na IS spracúvajúci osobné údaje z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

Cieľom auditu bude analyzovanie aktuálneho stavu segmentov informačného systému a porovnanie zisteného stavu so štandardami a relevantnými normami v národnom alebo medzinárodnom meradle.

Výsledkom analýzy bude rozpoznanie hrozieb, ktoré pôsobia na jednotlivé segmenty informačného systému v súčasnosti.

Audit bude zameraný na jednotlivé podskupiny IS spracúvajúce osobné údaje:
- bezpečnosť HW,
- bezpečnosť SW,
- bezpečnosť prostredia,
- logická kontrola prístupu a zodpovednosť za činnosť v systéme,
- spôsob zabezpečenia ochrany údajov.

Osobitná pozornosť bude venovaná preskúmaniu:
- dodržiavania zásad spracovania osobných údajov,
- ochrany práv dotknutých osôb,
- cezhraničného toku údajov,
- procesu spracovania osobných údajov (zverejňovanie, poskytovanie, sprístupňovanie, likvidovanie osobných údajov).

Audit sa skladá z nasledujúcich etáp:

1. etapa - Inicializácia auditu

Táto etapa sa presne a jednoznačne vymedzí predmet auditu. Stanoví kompetencie, zadefinuje podmienky prístupu k relevantným informáciám a podkladom. Hlavnou náplňou tejto časti je oboznámenie sa s prostredím, identifikácia spolupracovníkov a respondentov. Naplánovanie jednotlivých činností auditu.

2. etapa - Analýza súčasného stavu

Základným cieľom tejto etapy je identifikovanie súčasného stavu a aktuálnej dokumentácie a súvisiacich aktív. Rozsiahlosť a komplexnosť auditovaného informačného systému definuje možné prístupy k tejto etape. Východiskom bude existujúca dokumentácia Bezpečnostného projektu na ochranu osobných údajov.

3. etapa - Posúdenie aktuálnej úrovne bezpečnosti

Na základe pozorovania alebo priameho overenia, alebo rozhovorov s respondentmi, funkcií a mechanizmov bezpečnosti bude ohodnotená úroveň bezpečnosti a musí sa porovnať s požadovanou úrovňou. Výsledok tejto etapy je ohodnotenie a syntéza reálnej úrovne bezpečnosti.

4. etapa - Návrh odporúčaní

Náplňou tejto etapy je definovanie opatrení, ktoré je potrebné uviesť do praxe, aby bola dosiahnutá požadovaná úroveň bezpečnosti informačného systému.

5. etapa - Syntéza výsledkov

Výstupný dokument auditu môže obsahovať prezentáciu hodnôt, syntézu aktuálnej bezpečnosti, hlavné nedostatky bezpečnosti a s nimi súvisiace riziká a navrhované protiopatrenia.

Základným atribútom výsledku auditu je výrok, ktorý stanovuje kladné alebo záporné hodnotenie posudzovanej oblasti, systému alebo činností. Takéto vyjadrenie sa stanoví v súvislosti s porovnaním k známym požiadavkám, ku ktorým je porovnanie vztiahnuté. Získané výsledky analytických prác budú napokon slúžiť na vypracovanie hodnotiacej správy o výsledkoch auditu bezpečnosti IS Úradu normalizácie, metrológie a skúšobníctva SR v zmysle uvedeného zákona o ochrane osobných údajov.

Použitá metodika:

- COBIT (Control Objectives for Information and related Technology).

Požiadavky na organizáciu:

- sprístupnenie relevantných vnútropodnikových štandardov,
- poskytnutie všetkých relevantných požadovaných materiálov. Tieto podkladové materiály budú použité len na prípravu záverečných dokumentov, ktoré sú predmetom realizácie auditu.

Výstup:

- Správa z auditu bezpečnosti IS (na základe požiadaviek zákona č. 428/2002 Zb. o ochrane osobných údajov v znení neskorších predpisov).

3.2 Harmonogram

Práce na audite budú prebiehať podľa stanoveného harmonogramu. Po ukončení analytických prác budú spracované výstupné dokumenty. Tieto budú odovzdané pracovnej skupine. Po pripomienkovaní sa môže uskutočniť oponentské konanie k vzneseným pripomienkam. Akceptované pripomienky budú zapracované do záverečných materiálov a tieto budú odovzdané vedúcemu projektu obstarávateľa

Činnosť	**pracovné dni (od zahájenia)**
Prípravné práce	1
Definovanie pracovných skupín	1
Audit bezpečnosti informačného systému	2– 4
Spracovanie Hodnotiacej správy	3 – 6
Pripomienkovanie materiálov	7
Zapracovanie pripomienok	8
Odovzdanie záverečných materiálov	9

3.3 Cenová kalkulácia

Práce	Cena v EUR bez DPH
Fáza 1 prípravné práce, úvodné preskúmanie, zber vstupných materiálov, vedenie rozhovorov, analytické práce	15.680,-
Fáza 2 Spracovanie a posúdenie zhody a rozdielov vypracovanie hodnotiacej správy, Zapracovanie pripomienok, Finálne odovzdanie	14.260,-
Spolu	**29.940,-**

Obmedzenia časové:
Ponuka má platnosť 30 dní odo dňa jej predloženia.

V Bratislave, 17.12.2010

Milan Ďorda
senior manager

4. RIADENIE PROJEKTU

Naše dodávky sú riadené v súlade s požiadavkami normy ISO 9001:2000 na systém riadenia kvality. Certifikát na systém riadenia kvality sme získali pre oblasť "Projektovania a implementácie bezpečnostných systémov" a " Dodávanie a servis informačných systémov".

Projektové práce v oblasti bezpečnosti budú riadené skúsenými pracovníkmi držiteľmi certifikátu projektového riadenia podľa SPPR na základe STN EN ISO/IEC 17024 a podľa kritérií IPMA . V pozícii odborného garanta pre tento projekt bude držiteľ certifikátu CISA (Certified Information System Auditor).

Projektový manažment je filozofia prístupu k riadeniu projektu s jasne stanoveným cieľom, ktorý musí byť dosiahnutý v požadovanom čase, s určenými nákladmi a v požadovanej kvalite. Záujemca pri realizácii využíva tento osvedčený princíp. Naši projektoví manažéri majú dlhodobé skúsenosti z riadenia projektov vo viacerých inštitúciách, pričom vždy rešpektujú konkrétne špecifiká zákazníka.

V rámci projektu vykonávajú nasledujúce činnosti:

- riadia prácu príslušných strán na projekte a reportujú vedeniu projektu stav projektu, pričom sú zodpovední za detailné plánovanie, koordináciu a kontrolu všetkých činností, vykonávaných v rámci projektu,
- zodpovedajú za zabezpečenie zdrojov a kapacít, ktoré sú potrebné pre riadne vykonanie projektu a pre spoluprácu v rámci spoločných tímov pracujúcich na jednotlivých častiach projektu,
- majú právo ukladať úlohy a vyžadovať ich plnenie od pracovníkov navrhnutých zmluvnými stranami na spoluprácu v rámci spoločných pracovných tímov a pre riešenie jednotlivých častí výkonu,
- zodpovedajú za plnenie úloh, termínov a sledujú čerpanie rozpočtu v súlade so schváleným harmonogramom,
- zodpovedajú za zabezpečenie súčinnosti obstarávateľa a záujemcu pri poskytovaní údajov a schvaľovaní dokumentov v stanovených termínoch.

4.1 Formy riadenia projektu

Riadenie projektu sa bude riadiť metodikou podľa PMBOK Guide.

Obstarávateľ a uchádzač písomne menujú manažéra projektu za každú stranu. Manažér projektu je zodpovedný za priebeh a riadenie všetkých prác, ktoré budú predmetom zmluvy o dielo. Zároveň bude obstarávateľom aj záujemcom určený odborný garant, ktorý sa bude zúčastňovať stretnutí na základe požiadavky projektových manažérov.

Predmet plnenia zmluvy obsahuje dodávky prác, služieb, materiálov a strojov tak, ako vyplynuli z požiadaviek stanovených obstarávateľom, v nasledujúcich častiach:

Prípravné práce:

Cieľom bude vytvoriť spoločnú pracovnú skupinu, ktorá bude zodpovedná za prípravu podkladov, pripomienkovanie materiálov. Manažér projektu obstarávateľa oznámi písomne vedúcemu projektu záujemcu mená členov pracovnej skupiny. Pracovná skupina je riadená vedúcim projektu obstarávateľa. Úlohou členov pracovnej skupiny bude najmä:

- zodpovednosť za kvalitné a včasné vykonávanie pridelených úloh,
- aktívne sa zúčastňovať na stretnutiach pracovnej skupiny, na ktoré boli prizvaní,
- aktívne spolupracovať na riešení úloh a priebežných problémov,
- posudzovať a odsúhlasovať komplexné alebo čiastkové kroky navrhovaných riešení a dokumentov,
- konzultovať navrhované riešenia a postupy postupov s nadriadeným,
- spolupracovať a konzultovať navrhované riešenia s ďalšími zamestnancami svojho útvaru.

Z každého stretnutia pracovnej skupiny sa urobí písomný zápis so závermi, ktoré boli na stretnutí dohodnuté. Závery uvedené do zápisu sú záväzné pre pokračovanie prác. Stretnutie pracovnej skupiny organizuje a riadi manažér projektu obstarávateľa. Na stretnutiach pracovnej skupiny sa zúčastňuje manažér projektu záujemcu, podľa potreby môžu byť prizvaní odborní garanti ako i špecialisti záujemcu.

Požiadavky na obstarávateľa:

Úspešná realizácia plnenia predmetu zmluvy závisí aj od riadneho spolupôsobenia obstarávateľa v týchto oblastiach:

- písomné menovanie členov pracovnej skupiny,
- písomné menovanie manažéra projektu obstarávateľa,
- poskytnutie súčinnosti a podpory do 2 pracovných dní od zadefinovania požiadavky manažérovi projektu obstarávateľa,

Projektové práce sú riadené skúsenými pracovníkmi, kde medzi nich patria aj držitelia certifikátu projektového riadenia podľa SPPR na základe STN EN ISO/IEC 17024) a podľa kritérií IPMA ako i držitelia certifikátu CISM (Certified Information System Manager) pre oblasť bezpečnosti. Priebeh bezpečnostných projektov je vykonávaný pod dohľadom **interných audítorov** s **certifikátom CISA** (Certified Information System Auditor).

5. ZÁKLDNÉ ÚDAJE O SPOLOČNOSTI

Obchodný názov	**EMM, spol. s r. o.**
Vznik spoločnosti	1991
Sídlo	Sekurisova 16, 841 02 Bratislava
Telefón	+421 (2) 60254111
Fax	+421 (2) 60254901
E-mail	emm@emm.sk
Internet	http://www.emm.sk/
Štatutárne osoby	Ing. Mária Schill, štatutárny zástupca (konateľ) Ing. Jozef Chebeň, štatutárny zástupca (konateľ)
Registrácia	OS BA1, oddiel sro, vložka číslo 686/B
Peňažný ústav	ČSOB Bratislava
Číslo účtu	05 84749903/7500
IČO	17316260
IČ DPH	SK 2020316529

Kontakté údaje

Meno	Peter
Priezvisko	Belák
Funkcia	projektový manažér
Tel.č.	00421 2 602 54 111
Fax	00421 2 60254901
e-mail	belak@emm.sk

5.1 Predstavenie spoločnosti EMM, spol. s r.o.

Spoločnosť EMM, spol. s r. o. na slovenskom trhu pôsobí od roku 1991. Naša podnikateľská stratégia je založená na tvorbe informačných a bezpečnostných systémov od rôznych výrobcov. Chceme tým zabezpečiť Vašu technologickú nezávislosť, znížiť náklady na budovanie a poskytnúť veľkú flexibilitu pri ich inovácii a rozširovaní. Takáto stratégia kladie vysoké nároky na odborné znalosti našich zamestnancov. Preto investujeme do vzdelávania – naši zamestnanci sú experti so širokým teoretickými vedomosťami a bohatými praktickými skúsenosťami, ako prednášatelia sa zúčastňujú odborných seminárov či školení. Zároveň pomáhame vychovávať mladú generáciu odborníkov. Študentom vysokých škôl dávame možnosť overiť si teoretické znalosti v niektorých projektoch. Dosiahnuté úspechy nám však pripomínajú, že spoločensky a ekonomicky úspešný subjekt musí byť zároveň vnímavý k potrebám tých, ktorí sú odkázaní na pomoc a solidaritu, preto podporujeme charitatívnu činnosť.

Dnes už nik nepochybuje o tom, že správne a rýchle informácie sú základom pre správne rozhodovanie. Takéto informácie je možné zabezpečiť len pomocou organizovaného systému, v ktorom má každý komponent svoje úlohy a zabezpečený tok údajov. Je nemysliteľné zvládnuť takéto náročné úlohy bez špičkových technických riešení a služieb, ktoré sú v ponuke nášho úseku informačných systémov. Široké spektrum neustále sa doplňujúcich poznatkov našich školených a certifikovaných expertov nás zaraďuje do úzkej špičky firiem schopných budovať komplexné informačné systémy.

Podiel na kvalite našej práce majú aj svetové značky zvučných mien, s ktorými spolupracujeme. Sme dlhoročným autorizovaným obchodným partnerom firmy IBM. Aby na Vašom stole bolo všetko kompletné, dodávame, inštalujeme a servisujeme aj všetky doplnkové a spolupracujúce zariadenia. Servisujeme a dodávame produkty ďalšieho popredného svetového výrobcu – spoločnosti HP / COMPAQ, a to od výkonných 64-bitových systémov, cez celý sortiment PC techniky, až po veľkokapacitné pamäťové jednotky.

Realizujeme práce a ponúkame služby. **Realizovali sme úspešne** viaceré **projekty zamerané na ochranu osobných údajov v informačných systémoch našich zákazníkov**. Našimi zákazníkmi boli v tejto oblasti viaceré významné organizácie a finančné ústavy na slovenskom trhu. Pri realizácii bezpečnostných opatrení nezostávame len v oblasti ochrany osobných údajov. Rozhodujúcim faktorom pri využívaní zdrojov informačného systému je i proces identifikácie a autentifikácie, ktorý pri svojej práci využívajú používatelia, služby aj komponenty. Vo svojich projektoch preferujeme také prostriedky a metódy, ktoré minimalizujú možnosť zámeny identity, spochybnenie procesu autentifikácie a v konečnom dôsledku zneužitie zdrojov informačného systému. Naše riešenia sú založené na

použití symetrických a nesymetrických šifrovacích algoritmov, ktoré sú implementované softvérovými alebo hardvérovými prostriedkami. Jednotný identifikačný systém (JIS) chápeme ako riešenie, ktoré spĺňa požiadavku jediného identifikačného zariadenia (tokenu) vo všetkých oblastiach použitia (operačné systémy, databázové systémy, aplikácie, APV, riadenie fyzického prístupu).

Naše projekty a ich realizácia rešpektujú požiadavky vyplývajúce z noriem ISO, EÚ a Slovenskej republiky platnej pre oblasť identifikácie a bezpečnosti.

Na zabezpečenie požiadaviek JIS pre používateľov odporúčame používanie čipových kariet, ktoré sú integrované do prostredia operačných systémov a aplikácií. Nami ponúkané čipové karty (napr. Siemens, Datakey a Schlumberger) majú integrovanú podporu šifrovacích mechanizmov, spolupracujú s bežnými operačnými systémami a pomocou vývojového prostredia ich integrujeme aj do aplikácií tretích strán.

Nech si spomeniete na ktorúkoľvek oblasť informačných systémov, ponúkneme Vám len osvedčené značky. Tlačiarne od firiem XEROX, HP, IBM, OKI, Canon, Epson a TallyGenicom tvoria širokú škálu typov, technológií tlače, výkonnosti a účelu využitia. Ponúkame špeciálne modely od tlačiarní na tlač do vkladných knižiek, cez kvalitné laserové a atramentové tlačiarne, až po vysokovýkonné riadkové a laserové systémy. Ak hľadáte kvalitu v oblasti kancelárskej techniky, dodávame výrobky viacerých popredných svetových výrobcov, medzi ktorými samozrejme nesmie chýbať HP, XEROX, Canon a RICOH. V súčasnosti sa čoraz častejšie dostávajú k slovu digitálne kopírovacie a tlačiarenské systémy pre svoje bezkonkurenčné funkčné a ekonomické prednosti.

Aby bola naša ponuka kompletná, museli by sme ešte dlho pokračovať vo vymenovávaní. No nesmieme zabudnúť na nepretržité zdroje napájania, zálohovacie diskové, páskové, magnetooptické systémy, sieťové komponenty a všetky ďalšie periférne a doplnkové zariadenia, tvoriace spolu so softvérovými produktmi ucelené informačné systémy. Dodávky všetkých uvedených produktov zabezpečujeme celoplošným záručným aj pozáručným servisom. EMM, spol. s r. o. je držiteľom certifikátu riadenia kvality ISO 9001:2000.

5.2 Výhody spolupráce

Za výhodu spolupráce s našou firmou považujeme:

1. Znalosť prostredia a problematiky z projektov vedených vo finančných organizáciách, organizáciách štátnej a verejnej správy, výrobných podnikoch.

2. Vytvorenie koherentnej množiny opatrení v oblasti informačnej a technickej bezpečnosti tak, aby bola v budúcnosti možná integrácia s inými systémami, čo v konečnom dôsledku znamená vyššiu efektívnosť vynaložených prostriedkov.
3. Komplexné zabezpečenie analytických a realizačných prác v oblasti logickej (bezpečnosť informačného systému), technickej a režimovej bezpečnosti.
4. Používanie jednotnej metodiky projektovania bezpečnostných systémov v oblasti technickej bezpečnosti, režimovej bezpečnosti a bezpečnosti IS.
5. Znalosť problematiky riešenia projektov v oblasti čipových kariet, šifrovania a elektronického podpisu.
6. Overené metodiky auditu, analýzy rizík a návrhu bezpečnostnej architektúry, ktorá bola vypracovaná za účasti medzinárodných expertov.
7. Skúsenosti s implementáciou bezpečnostných opatrení v oblasti technickej a logickej bezpečnosti a ich integrácie do jednotného celku.
8. Skúsenosti s vypracovaním a realizáciou najväčších bezpečnostných projektov v SR.
9. Spolupráca s medzinárodnými expertmi.
10. Komplexné postupy zabezpečujúce posúdenie všetkých oblastí bezpečnosti, rovnomernú hĺbku posúdenia a konzistenciu výsledkov a návrhov.

V Bratislava, 17.12.2010

Milan Ďorda

senior manager