ZMLUVA O DIELO

Číslo u zhotoviteľa: 201312VA
Číslo u objednávateľa: TvU-2013-CIS-02

uzatvorená podľa §536 a nasl. zákona č. 513/1991 Z.z. Obchodný zákonník v znení neskorších predpisov

medzi

Zhotoviteľ:	Datasoft Consulting s.r.o. Baračka 87/85 91451 Trenčianske Teplice
Zastúpený:	Roman Václav - konateľ Datasoft Consulting s.r.o.
IČO:	36662739
IČ DPH:	
Bankové spojenie:	
Číslo účtu:	
Registrácia:	Obchodný register Okresného súdu Trenčín, oddiel: s.r.o., vložka číslo: 16964/R (ďalej len „zhotoviteľ“)
Objednávateľ :	Trnavská univerzita so sídlom v Trnave Hornopotočná 23, 918 43 Trnava
Zastúpený:	prof. doc. JUDr. Marek Šmid, PhD., rektor Trnavskej univerzity v Trnave
IČO:	31825249
IČO DPH:	
Bankové spojenie:	
Číslo účtu:	
	(ďalej len „objednávateľ“)

I. PREDMET ZMLUVY

1) Predmetom zmluvy je záväzok poskytovateľa vypracovať a dodať objednávateľovi:

   a) Dokumentáciu k Bezpečnostnému projektu na ochranu osobných údajov v zmysle zákona č. 122/2013 Z.z. o ochrane osobných údajov v znení neskorších predpisov a pokynov Úradu na ochranu osobných údajov, platných v čase tvorby diela;

   b) Dokumentáciu k Bezpečnostnej politike v zmysle zákona č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a v znení metodických pokynov MF SR;

   c) Licenciu softvérovej aplikácie na správu bezpečnostnej dokumentácie (ISSR) vrátane jej implementácie a podporných školení.

Presná špecifikácia predmetu zmluvy je uvedená v Prílohe č. 1 k tejto zmluve podľa úspešnej cenovej ponuky zo dňa 9. mája 2013. Predmet zmluvy odovzdá zhotoviteľ objednávateľovi v tlačenej podobe, na CD nosiči vrátane záverečnej prezentácie

v elektronickej forme a zároveň v naplnenej databáze funkčnej softvérovej aplikácie ISSR.

2) Objednávateľ sa zaväzuje zaplatiť cenu za riadne a včasne vykonané dielo v súlade s touto zmluvou .

3) Zhotoviteľ sa zaväzuje, že v prípade, ak počas doby plnenia nastane zmena legislatívy, ktorá bude mať vplyv na vypracovanú bezpečnostnú dokumentáciu o ochrane osobných údajov a informačnej bezpečnosti, bez zbytočného odkladu upozorní na tieto skutočnosti objednávateľa v písomnej forme. Po vzájomnej dohode bude dohodnutý postup zapracovania novej legislatívy do bezpečnostnej dokumentácie. V prípade potreby sa objednávateľ zúčastní na kontrolách inšpekčných orgánov kontrolných osôb u zhotoviteľa, ak bude na to objednávateľom vyzvaný. Odplata za služby v tomto bode sa dohodne pred zahájením práce podľa predpokladaného rozsahu činnosti dodatkom ku zmluve.

II. TERMÍN A MIESTO PLNENIA

1) Konečný termín splnenia predmetu zmluvy sa stanovuje do 100 pracovných dní odo dňa nadobudnutia účinnosti tejto zmluvy. Termíny plnenia jednotlivých častí predmetu zmluvy podľa článku I. ods.1 sú nasledovné:

   a) písm. a) do 60 pracovných dní od nadobudnutia účinnosti tejto zmluvy,
   b) písm. b) do 85 pracovných dní od nadobudnutia účinnosti tejto zmluvy,
   c) písm. c) do 100 pracovných dní od nadobudnutia účinnosti tejto zmluvy.

2) Miestom plnenia predmetu zmluvy sú všetky súčasti a pracoviská objednávateľa, v ktorých sa spracovávajú osobné údaje:

   a) Rektorát a Filozofická fakulta TU, Hornopotočná 23, 918 43 Trnava
   b) Pedagogická fakulta TU, Priemyselná 4, 917 01 Trnava
   c) Fakulta zdravotníctva a sociálnej práce TU, Univerzitné nám.1, 917 01 Trnava
   d) Teologická fakulta TU, Kostolná 1, 814 99 Bratislava
   e) Právnická fakulta TU, Kollárova 10, 917 01 Trnava
   f) Centrum Adalbertinum, Hollého 8, 917 01 Trnava

III. CENA ZA DIELO

1) Cena celkom za dielo je stanovená dohodou v zmysle zákona NR SR č. 18/1996Z.z. o cenách v znení neskorších predpisov vo výške 7 900 € (slovom sedemtisícdeväťsto €) bez DPH. Celková cena za dielo vrátane DPH 20 % je 9 480 € (slovom deväťtisícštyristoosemdesiat EUR). Cena je stanovená ako maximálna, vrátane všetkých nákladov zhotoviteľa.

2) Cena za dielo je rozdelená podľa jednotlivých častí predmetu zmluvy podľa článku I. ods.1 nasledovne:

   a) písm. a) cena bez DPH 2 400 €, cena s DPH 2 880 €,
   b) písm. b) cena bez DPH 2 200 €, cena s DPH 2 640 €,
   c) písm. c) cena bez DPH 3 300 €, cena s DPH 3 960 €.

IV. PLATOBNÉ PODMIENKY

1) Dohodnutú cenu čiastkových plnení podľa článku III. ods.2) tejto zmluvy uhradí objednávateľ zhotoviteľovi v lehote splatnosti do 30 dní od doručenia faktúry, ktorú je zhotoviteľ oprávnený vystaviť po písomnom protokolárnom odovzdaní a prevzatí príslušnej časti predmetu zmluvy formou akceptačného protokolu ku každej časti, podpísanom oprávnenými zástupcami zmluvných strán.

2) Oprávnenými zástupcami zmluvných strán sú:

   a) Za objednávateľa: doc.PhDr.Ing. Blanka Kudláčová, PhD., Ing. Jozef Koricina

   b) Za zhotoviteľa: Roman Václav, Mgr. Ján Sojka,

3) Faktúra vystavená poskytovateľom musí obsahovať zmluvne dohodnuté náležitosti, ako aj náležitosti v zmysle § 74 zákona č. 222/2004 Z.z. o dani z pridanej hodnoty v znení neskorších predpisov (ďalej len „zákon o DPH"), najmä :

   a) obchodné meno, sídlo, adresu objednávateľa,
   b) číslo faktúry,
   c) číslo zmluvy, na základe ktorej sa plní,
   d) označenie a názov predmetu diela (jeho časti),
   e) fakturovanú sumu,
   f) deň odoslania a deň zdaniteľného plnenia, dátum dodania služby
   g) dátum splatnosti,
   h) označenie peňažného ústavu a číslo účtu poskytovateľa, jeho IČO, IČ DPH, DRČ,
   i) pečiatku a podpis oprávnenej osoby poskytovateľa.

4) Pre prípad, že faktúra nebude obsahovať zmluvne dohodnuté a zákonom o DPH stanovené náležitosti, bude vystavená v neúplnom a v neprehľadnom stave, je objednávateľ oprávnený najneskôr do dňa jej splatnosti vadnú faktúru vrátiť poskytovateľovi na prepracovanie, pričom v sprievodnom liste uvedie vady faktúry. Nová lehota splatnosti takto prepracovanej faktúry sa riadi ustanovením ods. 1) tohto článku, pričom za dobu od vrátenia vadnej faktúry do dátumu splatnosti prepracovanej faktúry nie je Objednávateľ v omeškaní s jej úhradou.

V. ÚROK Z OMEŠKANIA, ZMLUVNÉ POKUTY

1) Ak zhotoviteľ poruší svoj záväzok tým, že riadne a v dohodnutých termínoch nevypracuje a neodovzdá objednávateľovi niektorú z častí predmetu zmluvy uvedenú v čl. I. ods.I a čl. II. ods.1 písm. a) až c) zmluvy a v Prílohe č.1 je objednávateľ oprávnený uplatniť si zmluvnú pokutu v percentuálnej výške ustanovenej v § 1 Nariadenia vlády SR č.21/2013 Z.z. z príslušnej čiastkovej ceny za dielo, uvedenej v čl. III. ods.2 tejto zmluvy.

2) Ak objednávateľ neuhradí čiastku za uskutočnené zdaniteľné plnenie v lehote splatnosti podľa čl. IV. ods. 1) tejto zmluvy, má poskytovateľ právo uplatniť úrok z omeškania v percentuálnej výške ustanovenej v § 1 Nariadenia vlády SR č.21/2013 Z.z. z fakturovanej ceny za každý deň omeškania po lehote splatnosti.

3) V prípade, že objednávateľ bude bezdôvodne narušovať dohodnuté pracovné stretnutia a v prípade, že objednávateľ neoznámi zhotoviteľovi najneskôr 1 deň pred plánovaným termínom pracovného stretnutia jeho zrušenie a pracovníci zhotoviteľa sa dostavia v dohodnutom termíne na pracovné stretnutie s objednávateľom a toto pracovné stretnutie sa neuskutoční z viny objednávateľa, môže zhotoviteľ účtovať objednávateľovi zmluvnú pokutu vo výške 100 € bez DPH za tento deň.

4) V prípade, že zamestnanci zhotoviteľa budú bezdôvodne narušovať dohodnuté termíny a v prípade, že zhotoviteľ neoznámi objednávateľovi najneskôr 1 deň pred plánovaným termínom pracovného stretnutia jeho zrušenie a pracovníci zhotoviteľa sa nedostavia v dohodnutom termíne na pracovné stretnutie s objednávateľom z viny zhotoviteľa, môže objednávateľ účtovať zhotoviteľovi zmluvnú pokutu vo výške 100,- € bez DPH za tento deň.

VI. ZÁVÄZKY ZMLUVNÝCH STRÁN

1) Objednávateľ sa zaväzuje:
   a) zabezpečiť spoluprácu zamestnancov objednávateľa so zamestnancami zhotoviteľa a zabezpečiť nevyhnutnú súčinnosť v rámci vopred dohodnutých pracovných stretnutí medzi zhotoviteľom a objednávateľom. Platí to aj pre dohodnuté pracovné stretnutia na vybraných pracoviskách objednávateľa. V prípade, že objednávateľ nezabezpečí splnenie tohto ustanovenia, posunie sa termín splnenia predmetu zmluvy o dobu, o ktorú došlo k časovému sklzu splnenia predmetu zmluvy.
   b) oznámiť zhotoviteľovi zrušenie plánovaného pracovného stretnutia najneskôr 1 deň pred týmto plánovaným pracovným stretnutím.
   c) brať na vedomie, akceptovať a riešiť oprávnené pripomienky zhotoviteľa o zistených skutočnostiach, ktoré by mohli výrazne ovplyvniť alebo ohroziť splnenie predmetu zmluvy.
   d) umožniť zamestnancom zhotoviteľa prístup do všetkých priestorov, k zariadeniam a požadovaným podkladom súvisiacim s predmetom zmluvy.
   e) po vzájomnej dohode a v rámci svojich možností zabezpečiť pre pracovníkov zhotoviteľa potrebný priestor, ktorý budú môcť v čase plnenia predmetu tejto zmluvy používať.

2) Zhotoviteľ sa zaväzuje:
   a) plniť a splniť predmet tejto zmluvy s odbornou starostlivosťou a v zmysle príslušných ustanovení zákona č. 122/2013Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, podporne zákona č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a v znení metodických pokynov MFSR v rozsahu diela.
   b) neposkytovať informácie o osobných údajoch objednávateľom spracovávaných, s ktorými príde do styku počas plnenia predmetu tejto zmluvy tretej osobe, ani ich nepoužiť v rozpore s ich účelom podľa tejto zmluvy pre svoje potreby. Ďalej sa zaväzuje, že bude takéto informácie chrániť aspoň v rovnakom rozsahu ako dôverné informácie vlastné s prihliadnutím na bezpečnostnú politiku objednávateľa. Povinnosť ochrany trvá aj po skončení platnosti tejto zmluvy.

c) dodržiavať termíny dohodnutých pracovných stretnutí medzi zhotoviteľom a objednávateľom.
d) oznámiť objednávateľovi zrušenie plánovaného pracovného stretnutia najneskôr 1 deň pred týmto plánovaným pracovným stretnutím.
e) chrániť vlastnícke práva objednávateľa a zachovávať dôvernosť pri priamych alebo sprostredkovaných informáciach, podkladoch a dokumentácii, ktorú obdržia jeho pracovníci. Zhotoviteľ sa zaväzuje dodržiavať mlčanlivosť o skutočnostiach, o ktorých sa dozvedel v súvislosti s plnením predmetu tejto zmluvy. V prípade, že objednávateľ hodnoverne preukáže porušenie tohto ustanovenia, je oprávnený domáhať sa vzniklej škody na zhotoviteľovi, na základe preukázania vzniku škody a výšky vzniklej škody znaleckým posudkom.
f) informovať objednávateľa o zistených skutočnostiach, ktoré by mohli výrazne ovplyvniť alebo ohroziť splnenie predmetu tejto zmluvy.

VII. ZÁRUKA, ZODPOVEDNOSŤ ZA VADY

1) Zhotoviteľ poskytuje na predmet zmluvy záruku 24 mesiacov od jeho protokolárneho prevzatia objednávateľom. Za odstránenie zistených vád v odozdanej dokumentácii a v softvérovej aplikácii ISSR nebude zhotoviteľ počas záručnej doby účtovať žiadnu odplatu.

2) Zhotoviteľ zodpovedá objednávateľovi za všetky škody, ktoré mu vzniknú z titulu dodávky vadného predmetu zmluvy. Zodpovednosť za vady sa riadi príslušnými ustanoveniami Obchodného zákonníka.

VIII. ODSTÚPENIE OD ZMLUVY

1) Zmluvné strany sa dohodli, že od zmluvy môžu odstúpiť pri podstatnom porušení zmluvných dojednaní v týchto prípadoch:

   a) Objednávateľ je v zmysle § 344 a § 345, ods.1 Obchodného zákonníka oprávnený jednostranne odstúpiť od zmluvy v prípade ak je zhotoviteľ v omeškaní s plnením predmetu zmluvy uvedeného v čl. I ods. 1 po dobu dlhšiu ako tri kalendárne mesiace po zmluvne dohodnutom termíne uvedenom v čl.II ods.1) a v prípade porušenia záväzkov zhotoviteľa uvedených v čl.VI. ods.2 písm a, b, e.

   b) Zhotoviteľ je oprávnený odstúpiť od zmluvy v prípade, že objednávateľ je v omeškaní s úhradou dohodnutej ceny podľa čl.III ods.2) dlhšie ako 30 (slovom tridsať) dní po lehote splatnosti doručenej faktúry.

2) Odstúpenie od zmluvy musí mať písomnú formu a nadobúda účinnosť okamihom jeho doručenia druhej zmluvnej strane.

3) Neplnenie predmetu zmluvy, zapríčinené vyššou mocou, nie je dôvodom k odstúpeniu od zmluvy, pokiaľ sa zmluvné strany nedohodnú inak.

4) Zmluvné strany sa dohodli, že za prípady vyššej moci budú považovať živelné pohromy, prírodné katastrofy, štrajky, embargá, administratívne opatrenia štátu a také iné udalosti, ktoré zmluvné strany ani pri najväčšej opatrnosti nemohli predvídať a ktorým pri použití obvyklých prostriedkov nemohli zabrániť.

5) Zmluvné strany sa dohodli, že platnosť zmluvy je možné ukončiť i dohodou zmluvných strán v písomnej forme.

IX. ZÁVEREČNÉ USTANOVENIA

1) Táto zmluva nadobúda platnosť dňom jej podpisu oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v zmysle § 47a zákona č. 40/1964 Zb. Občianskeho zákonníka v znení neskorších predpisov v spojení s § 5a zákona č. 211/2000 Z.z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Štatutárne orgány zmluvných strán podpisom tejto zmluvy vyjadrujú svoj súhlas s jej zverejním v plnom rozsahu.

2) Túto zmluvu možno zmeniť alebo doplňať len po dohode oboch zmluvných strán, a to výlučne písomným(ými) dodatkom(ami), schváleným(mi) a podpísaným(mi) oprávnenými zástupcami oboch zmluvných strán. Zmluvné strany vylučujú odklon od tejto požiadavky ústnym alebo konkludentným spôsobom. Vedľajšie ústne dohody nemajú žiadne právne následky.

3) Zmluvné strany sa zaväzujú, že vyvinú maximálne úsilie a tvorivú spoluprácu na zmluvné zabezpečenie predmetu zmluvy. Prípadné spory súvisiace s touto zmluvou vyriešia zmluvné strany rokovaním na základe vzájomnej dohody. Pre prípad, že nedôjde k dohode a k zmiernemu riešeniu, je oprávnená ktorákoľvek zo zmluvných strán uplatniť svoj nárok súdnou cestou na príslušnom súde v zmysle príslušných ustanovení O.s.p.

4) Táto zmluva je vyhotovená v štyroch rovnopisoch, pre každú zmluvnú stranu sú určené dva rovnopisy.

5) Vzťahy, touto zmluvou výslovne neupravené, sa budú riadiť príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi, všeobecne záväznými právnymi predpismi Slovenskej republiky.

6) V prípade, ak niektoré ustanovenie tejto zmluvy je alebo sa stane neplatným či neúčinným, nedotýka sa to ostatných ustanovení tejto zmluvy, ktoré zostávajú platné a účinné. Zmluvné strany sa v takom prípade zaväzujú dodatkom k tejto zmluve nahradiť neplatné či neúčinné ustanovenie ustanovením platným či účinným, ktoré čo najlepšie zodpovedá pôvodne zamýšľanému účelu ustanovenia neplatného čí neúčinného. Do uzavretia takého dodatku platí zodpovedajúca právna úprava všeobecne záväzných právnych predpisov Slovenskej republiky.

7) Neoddeliteľnou súčasťou zmluvy je Príloha č.1 Obsahová špecifikácia predmetu zmluvy.

8) Zmluvné strany prehlasujú, že si zmluvu prečítali, jej obsahu porozumeli a na znak súhlasu s jej znením ju vlastnoručne oprávnenými zástupcami zmluvných strán podpísali.

V Trnave , dňa :

V Trenčianskych Tepliciach, dňa :

Za objednávateľa: .....
prof.doc.JUDr. Marek Šmid, PhD.
rektor Trnavskej univerzity v Trnave

Za zhotoviteľa:.....
Roman Václav
konateľ Datasoft Consulting s.r.o.

Príloha č.1

OBSAHOVÁ ŠPECIFIKÁCIA PREDMETU ZMLUVY

Služby na činnosti súvisiace s ochranou osobných údajov a bezpečnosťou informačných systémov Trnavskej univerzity

1. BEZPEČNOSTNÝ PROJEKT :

A) bezpečnostný zámer
- základné bezpečnostné ciele
- technické, organizačné a personálne opatrenia na zabezpečenie ochrany OÚ v informačných systémoch prevádzkovateľa
- vymedzenie okolia IS v súvislosti s možným narušením ochrany OÚ v informačných systémoch prevádzkovateľa

B) analýza bezpečnosti
- identifikácia všetkých IS, v ktorých sa spracúvajú osobné údaje dotknutých osôb u prevádzkovateľa
- identifikácia prostredia prevádzkovaných informačných systémov (fyzický priestor, technické prostriedky spracúvania, ostatné technické prostriedky)
- vytvorenie zoznamu aktív, zraniteľností, hrozieb a ich ohodnotenie
- identifikácia a kvalitatívna analýza relevantných rizík a ich ohodnotenie
- návrh ochranných opatrení na elimináciu identifikovaných rizík

C) bezpečnostné smernice
- smernica na zabezpečenie prevádzky informačných systémov
- pravidlá manipulácie s citlivými dátami
- smernica na ochranu osobných údajov
- plány na riešenie havarijných stavov informačných systémov

Plnenie definovaných kritérií :

Normy, z ktorých sa vychádza pri spracovaní dokumentácie:

Pre vypracovanie bezpečnostnej dokumentácie na ochranu osobných údajov zhotoviteľ vychádza z požiadaviek národnej legislatívy, teda v čase tvorby ponuky platného zákona na ochranu osobných údajov č. 428/2002 Z.z. v znení neskorších predpisov. V prípade realizácie diela pri súčasnej zmene legislatívy sa bude dielo realizovať podľa aktuálne platnej legislatívy. Ďalej je východiskom súbor medzinárodných štandardov pre systémy riadenia informačnej bezpečnosti ISO 27001 a súvisiacich predpisov a z požiadaviek výnosu MF č.312/2010 pre bezpečnosť ISVS §28 až. §42.

Spôsob získavania informácií k spracovaniu príslušnej dokumentácie:

Pri vypracovaní bezpečnostnej dokumentácie na ochranu OÚ je najdôležitejšou podmienkou správna a jednoznačná identifikácia všetkých informačných systémov, v ktorých prevádzkovateľ spracúva OÚ v zmysle zákona č. 428/2002 Z.z. Ďalej nasleduje podrobný popis jednotlivých informačných systémov . Táto fáza tvorby projektu je analytickou fázou, ktorá spočíva v získavaní požadovaných informácií prostredníctvom vopred pripravených

dotazníkov zhotoviteľa. Poverený zástupca prevádzkovateľa obdrží od audítora súbor otázok ku konkrétnym skutočnostiam v elektronickej forme, ktoré v spolupráci s poverenými oprávnenými osobami vyplní podľa pokynov na dotazníku. Následne pokračuje analytická časť osobnými konzultáciami audítora s oprávnenými osobami poskytujúcimi informácie na ich detailizácii tak, aby sa spresnili jednotlivé odpovede a odstránili prípadne nejasnosti. Po absolvovaní rozhovorov dostanú jednotlivé oprávnené osoby, ktoré poskytli informácie, dotazníky na ich verifikáciu, kde svojim podpisom potvrdzujú správnosť poskytnutých informácií. (Jeden rovnopis zostáva zamestnancovi, jeden rovnopis získa prevádzkovateľ ako súčasť projektovej dokumentácie a jeden rovnopis je pre zhotoviteľa)

Rozsah dotazníkov k analytickej časti projektu :

Identifikácia informačných systémov. V tejto časti sa zisťujú podrobné informácie o informačných systémoch, v ktorých prevádzkovateľ spracúva OÚ. Dotazník okrem iných obsahuje nasledovné údaje: Názov informačného systému, Zoznam spracúvaných osobných údajov, Zoznam spracúvaných kópii osobných dokladov, Spôsob získavania OÚ, Právny základ IS, Oprávnené osoby, Okruh dotknutých osôb, Sprístupňovanie OÚ z IS, Poskytovanie OÚ z IS, Zverejňovanie OÚ z IS, Prenos OÚ do tretích krajín, Sprostredkovatelia pre spracovanie OÚ z IS, Automatizované prostriedky spracúvania, Neautomatizované prostriedky spracúvania, Umiestnenie IS Automatizovaná forma, Umiestnenie IS neautomatizovaná forma, Logický prístup k automatizovanej forme spracovania.

Každý popis k identifikovanému informačnému systému obsahuje fyzické umiestnenie dát z informačného systému, pričom je zachované individuálne členenie na automatizované dáta a neautomatizované dáta. Z týchto informácií sa generuje zoznam fyzických miest s umiestnením dát z jednotlivých IS. Pre každé fyzické miesto uloženia dát sa vytvára dotazník získavajúci informácie o tomto konkrétnom umiestnení. (Popis fyzického prostredia , použité technické prostriedky na spracovanie v tomto mieste, prijate bezpečnostné opatrenia....). Ďalej popis IS obsahuje informáciu o logickom prístupe k dátam jednotlivých IS. Z tejto informácie vzniká zoznam miest logického prístupu. Každý logický prístup generuje dotazník s informáciami obsahujúcimi popis jednotlivého miesta. Získavajú sa nasledovné informácie: Popis fyzického prostredia, použité technické prostriedky, spôsob autorizácie oprávnených osôb, prijate ochranné opatrenia.

Všetky informácie z analytickej časti tvorby bezpečnostnej dokumentácie sú nevyhnutným predpokladom na spracovanie správnej a konkrétnej analýzy bezpečnosti informačných systémov u prevádzkovateľa

Predpokladaný zoznam dokumentov:

Dotazníková štruktúra analytickej časti vyzerá nasledovne:

Dokument obsahujúci zoznam informačných systémov

- Dokumenty obsahujúce informácie o IS 1 až IS X

Dokument obsahujúci zoznam fyzického umiestnenia dát IS

- Dokument obsahujúci popis miesta 1 až X

Dokument obsahujúci zoznam logických prístupov k dátam jednotlivých IS

- Dokument obsahujúci informácie o logickom prístupe 1 až X

Dokument obsahujúci zoznam areálov, v ktorých sa nachádzajú dáta jednotlivých IS.
Dokument obsahujúci zoznam budov v jednotlivých areáloch, v ktorých sa nachádzajú dáta jednotlivých IS.
Dokument obsahujúci informácie o úrovni implementácie cieľov riadenia IB podľa ISO 27001.
Z vyššie uvedených dotazníkov analytickej časti, bude vypracovaná bezpečnostná dokumentácia, ktorá bude obsahovať nasledovné dokumenty:

1. Bezpečnostný zámer
2. Analýza bezpečnosti
3. Bezpečnostné smernice
4. Zoznam oprávnených osôb
5. Zoznam zodpovedných osôb
6. Zoznam sprostredkovateľov
7. Vzor poučenia oprávnených osôb.
8. Vzor poverenia zodpovednej osoby.
9. Vzor súhlasu so spracúvaním OÚ.
10. Vzor súhlasu so spracúvaním OD.(osobného dokladu)
11. Evidenčné listy jednotlivých IS. (Prípadne registračné listy ak sa pre daný IS vyžaduje registrácia, alebo osobitná registrácia)
12. Zoznam dôležitých procesov súvisiacich zo spracúvaním OÚ.

Stručný obsah anotácia jednotlivých dokumentov:

1. **Bezpečnostný zámer** – Obsahuje základné bezpečnostné ciele, teda informáciu o tom čo požaduje prevádzkovateľ v oblasti ochrany osobných údajov. Ďalej zámer obsahuje informácie o prijatých a plánovaných ochranných opatreniach. Detailný popis jednotlivých informačných systémov minimálne v rozsahu evidenčného listu IS. Popis technických prostriedkov použitých na spracovanie OÚ. Popis prostredia v ktorom sa spracúvanú OÚ.

2. **Analýza bezpečnosti** – Obsahuje zoznam aktív, zraniteľnosti, hrozieb z toho generovaných rizík, zoznam dopadov rizík a zoznam ochranných opatrení (implementovaných a navrhovaných). Všetky prvky sú ohodnotené na základe stanovených kritérií hodnotenia. Výsledkom analýzy je zoznam zostatkových rizík, nepokrytých rizík a ochranných opatrení.

3. **Bezpečnostné smernice**- Popisujú spôsob implementácie jednotlivých ochranných opatrení či už implementovaných, alebo navrhovaných opatrení, so špecifikáciou zodpovednosti za implementáciu jednotlivých opatrení. Definujú práva a povinnosti oprávnených osôb, práva a povinnosti zodpovedných osôb, práva a povinnosti prevádzkovateľa, vzťah prevádzkovateľ - sprostredkovateľ ak existuje. Postupy pri autorizácii prístupu k IS, postupy pri riešení havarijných stavov, postupy pri riešení incidentov OÚ.

4. **Zoznam oprávnených osôb** – Obsahuje informáciu o oprávnených osobách pre jednotlivé IS o ich oprávneniach prípadne obmedzeniach pri spracúvaní OÚ v IS.
5. **Zoznam zodpovedných osôb** – Obsahuje informáciu o zodpovedných osobách pre jednotlivé IS a o ich povinnostiach.
6. **Zoznam sprostredkovateľov** – Obsahuje informáciu o sprostredkovateľoch poverených spracúvaním OÚ v IS prevádzkovateľa. Spôsob poverenia, rozsah poverenia, podmienky spracúvania OÚ.
7. **Vzor poučenia oprávnených osôb.** – Obsahuje návrh obsahu a formy poučenia OÓ.
8. **Vzor poverenia zodpovednej osoby.** – Obsahuje návrh obsahu a formu poverenia zodpovednej osoby s informáciou o povinnostiach zodpovednej osoby.
9. **Vzor súhlasu so spracúvaním OÚ.**- Obsahuje návrh a formu súhlasu so spracúvaním OÚ.
10. **Vzor súhlasu so spracúvaním OD.(osobného dokladu)** - Obsahuje návrh a formu súhlasu so spracúvaním OD.
11. **Evidenčné listy jednotlivých IS. (Prípadne registračné listy ak sa pre daný IS vyžaduje registrácia, alebo osobitná registrácia)** – Obsah v zmysle zákona č428/2002 Z.z na ochranu OÚ.
12. **Zoznam dôležitých procesov súvisiacich zo spracúvaním OÚ.** – Obsahuje zoznam a popis jednotlivých procesov súvisiacich so spracúvaním OÚ (Proces získavania OU, Proces likvidácie OÚ, ...)

Predpokladaná časová lehota :

- záleží od súčinnosti oprávnených osôb prevádzkovateľa. Predpokladaná lehota plnenia je 60 pracovných dní (osobodní)

Školenie pre oprávnené osoby :

súčasťou implementácie bezpečnostnej dokumentácie bude aj školenie pre oprávnené osoby prevádzkovateľa, ktoré sa bude konať vo vybraných priestoroch prevádzkovateľa.

Rozsah školenia , cca 8 hodín:

1. Legislatívne požiadavky na ochranu osobných údajov v podmienkach SR vrátane súhrnu hlavných zmien v novej legislatívnej úprave a časové lehoty na zosúladenie s požiadavkami novej legislatívnej úpravy.
2. Definície základných pojmov ochrany OÚ, povinnosti prevádzkovateľa, povinnosti zodpovednej osoby, atď
3. Bezpečnostný projekt a smernice na ochranu osobných údajov v rozsahu :

3a, informačné systémy, v ktorých SP spracúva osobné údaje dotknutých osôb,

dôkladné vysvetlenie všetkých informačných systémov

3b, Právny základ spracúvania OÚ., vedenie evidencie IS a ich registrácia

3c, rozsah bezpečnostnej dokumentácie

4. Práva dotknutých osôb.
5. Požiadavky na systém ochrany OÚ (bezpečnostné smernice, bezpečnostný projekt, ochranné opatrenia)
6. Úrad na ochranu OÚ – postavenie, kontrolná a metodická činnosť
7. Informačná bezpečnosť v systéme riadenia ochrany osobných údajov
8. Nástroje na automatizovanú správu dokumentácie zjednodušujúce dohľad nad ochranou OÚ u prevádzkovateľa

2. BEZPEČNOSTNÁ POLITIKA :

A. Pravidlá bezpečnostnej politiky

- bezpečnostná dokumentácia na zdokumentovanie prijatých bezpečnostných opatrení s rozsahom oprávnení a zodpovednosti
- definícia štandardov technických opatrení na bezpečnosť informačných systémov
- organizačné opatrenia a postupy na zavedenie bezpečnostnej politiky do praxe

B. Plán implementácie BP

C. Školenia pre oprávnené osoby a zodpovednú osobu za ochranu osobných údajov

D. Plán kontrolnej činnosti pri zavádzaní BP do praxe

Normy, z ktorých sa vychádza pri spracovaní dokumentácie:

Pri vypracovaní bezpečnostnej politiky sa vychádza v prvom rade z požiadaviek zákona o ISVS a z požiadaviek výnosu MF č.312/2010 pre bezpečnosť ISVS §28 až. §42. a medzinárodného štandardu pre systémy riadenia informačnej bezpečnosti ISO 27001.

Spôsob získavania informácií k spracovaniu príslušnej dokumentácie:

Informácie potrebné pre vypracovanie bezpečnostnej politiky organizácie sa získavajú formou osobných rozhovorov s jednotlivými zamestnancami zodpovednými za príslušnú oblasť riadenia informačnej bezpečnosti.

Ako podklad pre vypracovanie politiky IB slúži aj dotazník s názvom „Stav implementácie ochranných opatrení slúžiacich na dosiahnutie vybraných cieľov riadenia podľa ISO 27001 a požiadaviek výnosu MF č. 312/2010." Dotazník obsahuje otázky na popis stavu implementácie opatrení v nasledovných oblastiach riadenia IB:

- Bezpečnostná politika
- Organizačná bezpečnosť
- Klasifikácia a riadenie aktív
- Personálna bezpečnosť

- Fyzická bezpečnosť a bezpečnosť prostredia
- Riadenie komunikácie a prevádzky
- Riadenie prístupu
- Vývoj a údržba
- Riadenie kontinuity činnosti
- Súlad

Predpokladaný zoznam dokumentov:

Politika IB bude pozostávať z nasledovných dokumentov:

- Vyhlásenie politiky IB organizácie.
- Bezpečnostná politika
- Politika organizácie bezpečnosti
- Politika klasifikácie a riadenia aktív
- Politika personálnej bezpečnosti
- Politika fyzickej bezpečnosti a bezpečnosti prostredia
- Politika riadenia komunikácie a prevádzky
- Politika riadenia prístupu
- Politika vývoja a údržby
- Politika riadenia kontinuity činnosti organizácie
- Politika súladu

Stručný obsah anotácia jednotlivých dokumentov:

- **Vyhlásenie politiky IB organizácie.** – obsahuje definovanie bezpečnostných cieľov organizácie, stanovenie a deklaráciu úlohy manažmentu v podpore budovania systému riadenia informačnej bezpečnosti.
- **Bezpečnostná politika.** – obsahuje spôsob vyhodnocovania dosiahnutia bezpečnostných cieľov, kritéria vyhodnocovania, spôsob priebežného hodnotenia. Spôsob schvaľovania politiky IB. Periodicity vykonávania revízie politiky IB.
- **Politika organizácie bezpečnosti**. – obsahuje riešenie problematiky infraštruktúry IB, určenie všeobecných a špecifických zodpovedností za jednotlivé oblasti IB. Definovanie manažérskych pozícii pre oblasť riadenia IB. Rieši problematiku prístupu tretích strán.
- **Politika klasifikácie a riadenia aktív.** – rieši problematiku klasifikácie aktív (vytvorenia zoznamu aktív organizácie ktoré je potrebné chrániť) definuje spôsob vyhodnocovania a kritéria hodnotenia aktív. Určenie zodpovednosti za jednotlivé aktíva. Definovanie rámca pre manažment rizík. Stanovenie požiadaviek na vykonávanie analýzy rizík a jej revízie.
- **Politika personálnej bezpečnosti.** – definuje problematiku činnosti vyžadovaných pri primaní nových zamestnancov, počas trvania pracovného vzťahu a pri ukončení pracovného vzťahu. Definuje požiadavky na vzdelávanie a budovanie povedomia

IB. Definuje požiadavky na manažment incidentov, spôsob nahlasovania incidentov a bezpečnostných slabýn.

- **Politika fyzickej bezpečnosti a bezpečnosti prostredia.** – definuje požiadavky na vytvorenie fyzických okruhov rôzneho stupňa zabezpečenia, s definovaním podmienok autorizácie pre jednotlivé okruhy a požiadaviek na umiestňovanie aktív v príslušných okruhoch. Stanovuje podmienky na zabezpečenie jednotlivých okruhov. Obsahuje požiadavky na údržbu zariadení, podmienky bezpečnej dodávky el. energie.
- **Politika riadenia komunikácie a prevádzky.** – obsahuje požiadavky na popis prevádzkových procesov, požiadavky v oblasti plánovania kapacít jednotlivých systémov. Požiadavky na ochranu voči škodlivému SW, problematika riadení sieti a nakladania s dátovými nosičmi.
- **Politika riadenia prístupu.** – Definuje požiadavky v oblasti riadenia prístupu, spôsob a forma prideľovania, revidovania a odoberania prístupov k aktívam organizácie. Požiadavky na riadenie prístupových hesiel.
- **Politika vývoja a údržby.** – Definuje požiadavky na činnosti pri vývoji systémov, oddelenie vývojového prostredia od bežnej prevádzky, požiadavky na používanie kryptografických opatrení.
- **Politika riadenia kontinuity činnosti organizácie.** – Definuje požiadavky na manažment kontinuity činnosti organizácie, stanovuje pravidla pre definovanie a ohodnotenie havarijných stavov, požiadavky na vypracovanie havarijných plánov a plánov obnovy kontinuity činnosti.
- **Politika súladu.** – Definuje požiadavky na spôsob udržiavania organizácie v súlade so všeobecne záväznými právnymi predpismi , zmluvnými záväzkami a vnútornými predpismi organizácie.
- **Špecifikácia použiteľnosti.** – Zhodnotenie stavu použitia prípadne vylúčenia požiadaviek normy ISO 27001 pre oblasť cieľov riadenia a odporúčaných opatrení pre dosiahnutie vybraných cieľov riadenia.

Predpokladaná časová lehota :

- záleží od súčinnosti oprávnených osôb prevádzkovateľa. Predpokladaná lehota plnenia je 60 pracovných dní (osobodní)

Školenie pre poverené oprávnené osoby :

súčasťou implementácie bezpečnostnej dokumentácie bude aj školenie pre poverené osoby prevádzkovateľa, ktoré sa bude konať vo vybraných priestoroch prevádzkovateľa.

Rozsah školenia , cca 8 hodín:

1.**Legislatívne požiadavky na systémy riadenia informačnej bezpečnosti pre povinné osoby**

2.**Medzinárodné štandardy z ktorých vychádzajú systémy riadenia informačnej bezpečnosti.** (ISO/IEC 27001,27002, ISO 13335 1-5)

3.**Definícia základných pojmov informačnej bezpečnosti** (Aktívum, hrozba, zraniteľnosť, riziko, miera rizika, dopad, zostatkové riziko...) a ich aplikácia u povinnej osoby

4. **Výnos MFSR 312/2010 Z.z. o štandardoch pre informačné systémy verejnej správy** (ISVS) v znení neskorších predpisov (MF/012943/2012-16 o hodnotení bezpečnostných štandardov)

- §28 štandardy pre riadenie informačnej bezpečnosti.
- §29 personálna bezpečnosť.
- §30 manažment rizík pre oblasť informačnej bezpečnosti.
- §31 kontrolný mechanizmus riadenia informačnej bezpečnosti.
- §32 ochrana proti škodlivému kódu.
- §33 sieťová bezpečnosť.
- §34 fyzická bezpečnosť a bezpečnosť prostredia.
- §35 aktualizácia softvéru.
- §36 monitorovanie a manažment bezpečnostných incidentov.
- §37 periodické hodnotenie zraniteľnosti.
- §38 zálohovanie.
- §39 fyzické ukladanie záloh.
- §40 riadenie prístupu.
- §41 aktualizácia informačno - komunikačných technológii.
- §42 účasť tretej strany.

5. **Metodiky analýzy rizík**

6. **Interné audity** systému riadenia informačnej bezpečnosti. Požiadavky na audit a požiadavky na interných audítorov

Súčasťou realizácie tejto časti diela – bezpečnostnej politiky - bude vypracovanie plánu implementácie bezpečnostnej dokumentácie vrátane plánu kontrolnej činnosti pri zavádzaní pravidiel bezpečnostnej politiky do praxe. Zároveň poskytneme metodiku k realizácii interného auditu v oblasti ochrany osobných údajov a informačnej bezpečnosti tak, aby poverená osoba prevádzkovateľa mohla samostatne vykonávať auditnú činnosť v organizácii.

3. SYSTÉM AUTOMATIZOVANEJ SPRÁVY BEZPEČNOSTNEJ DOKUMENTÁCIE - ISSR :

A. Licenčné podmienky pre softvérovú aplikáciu na zjednodušenie a sprehľadnenie implementácie systému riadenia informačnej bezpečnosti

B. Riadený prístup pre poverených používateľov

C. Popis jednotlivých modulov

Naša spoločnosť je autorom softvérovej aplikácie **ISSR – integrovaná správa systémov riadenia**, ktorá sa skladá z viacerých modulov, pričom jej primárnym cieľom je automatizovaná správa bezpečnostnej dokumentácie, s riadeným prístupom nielen k dokumentácii, ale aj k aktívam spoločnosti.

Licenčné podmienky pre Trnavskú univerzitu ako autor aplikácie poskytneme na časovo neobmedzené používanie licencie v počte : 1 serverová licencia + počet užívateľských licencií rovnajúci sa počtu oprávnených osôb poskytovateľa v definovanej verzii aplikácie ISSR (teda minimálne 72 užívateľských licencií)

Implementácia aplikácie prebehne v užívateľskom prostredí Trnavskej univerzity.

Súčasťou prác na úspešnej implementácii aplikácie je naplnenie databáz dátami z Bezpečnostného projektu a bezpečnostnej politiky v zmysle tejto ponuky.

Aplikácia funguje v prostredí operačného systému Windows XP a vyšší. Databáza MS SQL 2005 .

Aplikácia ISSR garantuje riadený prístup užívateľov k jednotlivým modulom aplikácie.

ISSR - moduly

Aplikácia ISSR bude pre Trnavskú univerzitu pozostávať zo 4 modulov :

1. modul Ochrana osobných údajov
2. modul Informačná bezpečnosť
3. modul interný audit - pravidlá
4. modul legislatíva

Súčasťou modulov 1 a 2 (ochrana osobných údajov a informačná bezpečnosť) je riadený prístup k bezpečnostnej dokumentácii, takisto riadený prístup k databáze aktív – informačným systémom, v ktorých spracúva prevádzkovateľ osobné údaje, zoznamom oprávnených osôb, ich vzájomných väzieb, zároveň umožňuje správu a vedenie databáz prvkov IB : aktív, zraniteľností, hrozieb, rizík, dopadov, ochranných opatrení, dokumentáciu procesov a prevádzkových záznamov, manažment rizík a vykonávanie analýz rizík, manažment incidentov a manažment riadenia kontinuity procesov a mnoho ďalších prvkov v oblasti informačnej bezpečnosti

Modul 3 AUDIT obsahuje konkrétne metodiky na vykonávanie interného auditu

Modul 4 LEGISLATÍVA obsahuje aktuálne platnú národnú legislatívu k ochrane osobných údajov a informačnej bezpečnosti + výber medzinárodných noriem a predpisov.

Aplikácia ISSR je v súlade s medzinárodnými štandardmi v oblasti riadenia informačnej bezpečnosti a zároveň národnou legislatívou , so zákonom č. 275/2006 o ISVS , výnosmi a metodikami MF SR a zákonom č. 428/2002 Z.z. o ochrane osobných údajov , v znení neskorších predpisov.

Modularita aplikácie ISSR :

Tento produkt je využiteľný a rozšíriteľný v moduloch pre všetky systémy riadenia, teda okrem informačnej bezpečnosti a ochrany osobných údajov aj o moduly enviroment, systém riadenia kvality a BOZP, teda je určený pre všetky integrované manažérske systémy riadenia.

ISSR vieme prispôsobiť špeciálnym požiadavkám koncového používateľa, keďže sme jej autorom, vrátane individuálnej licenčnej politiky.

Aktualizácia licencií a podpora pre prevádzku ISSR pre Trnavskú univerzitu :

- bezplatná podpora a aktualizácia počas 12 mesiacov od implementácie.
- voliteľná platená podpora a aktualizácia vo výške max. 12% obstarávacích nákladov / ročne po uplynutí bezplatnej podpory

V Trnave , dňa :

V Trenčianskych Tepliciach, dňa :

Za objednávateľa: .....
prof.doc.JUDr. Marek Šmid, PhD.
rektor Trnavskej univerzity v Trnave

Za zhotoviteľa:.....
Roman Václav
konateľ Datasoft Consulting s.r.o.