

ZMLUVA O DIELO A LICENČNÁ ZMLUVA

Číslo u zhotoviteľa: 201321VA

uzatvorená v zmysle ustanovení 269 a nasl. a § 536 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a ustanovení zákona č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon) v znení neskorších predpisov (ďalej len „zmluva“)

I. ZMLUVNÉ STRANY

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: SK2022229924
Bankové spojenie: ČSOB a.s.
Číslo účtu: 4013777247/7500
Registrácia: Obchodný register Okresného súdu Trenčín, Vložka číslo: 16964/R
(ďalej len „zhotoviteľ“)

Objednávateľ : IUVENTA – Slovenský inštitút mládeže
Zastúpený: Ing. Viliam Michalovič
IČO: 00157660
DIČ: 2020798637
Bankové spojenie: Štátna pokladnica, Bratislava
Číslo účtu: 7000123811 / 8180
(ďalej len „objednávateľ“)

II. PREDMET ZMLUVY

1. Predmetom zmluvy je záväzok poskytovateľa vypracovať a dodať objednávateľovi:
 - 1.1. bezpečnostný projekt, ako systém riadenia ochrany osobných údajov v pôsobnosti objednávateľa, podľa ustanovení zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení, platných v čase tvorby bezpečnostného projektu a metodikami, ktoré boli určené zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a jeho vykonávacími právnymi predpismi,
 - 1.2. nastavenie pravidiel bezpečnosti IS
 - 1.3. preškolenie oprávnených osôb
 - 1.4. Podpora a konzultácie k systému IB 26 mesiacov
 - 1.5. Príprava zodpovednej osoby na skúšky
 - 1.6. Podpora pri internom a externom audite
 - 1.7. licenciю softvérovej aplikácie na správu bezpečnostnej dokumentácie (ISSR) vrátane jej implementácie
(ďalej len „dielo“).
2. Presná špecifikácia predmetu zmluvy je uvedená v Prílohe č. 1 k tejto zmluve.

3. Predmet zmluvy odovzdá zhotoviteľ objednávateľovi v tlačenej podobe v počte 1 kus, na CD nosiči (súbor vo formáte pdf), vrátane záverečnej prezentácie v elektronickej forme a zároveň v naplnenej databáze funkčnej softvérovej aplikácie ISSR.
4. Objednávateľ sa zaväzuje zaplatiť cenu za riadne a včasne vykonané dielo v súlade s touto zmluvou.
5. 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 zhotoviteľ zúčastní na kontrolách inšpekčných orgánov kontrolných osôb u objednávateľa, ak bude na to objednávateľom vyzvaný.
6. Oprávnený zástupca na odovzdanie za zhotoviteľa : Roman Václav
Oprávnený zástupca na prevzatie za objednávateľa : Vladimír Kollár

III. TERMÍN A Miesto PLNENIA

1. Zhotoviteľ sa zaväzuje zhotoviť dielo najneskôr do 31.12.2015
2. Dielo bude zhotoviteľovi odovzdané na základe preberacieho protokolu.
3. Miestom plnenia predmetu zmluvy sú všetky súčasti a pracoviská objednávateľa, v ktorých sa spracovávajú osobné údaje:
 - a) Búdková 2, Bratislava
 - b) Karloveská 64, Bratislava
 - c) Tematické centrum mládeže, Košice
 - d) Tematické centrum mládeže, Prešov
 - e) Tematické centrum mládeže, Žilina
 - f) Tematické centrum mládeže, Banská Bystrica
 - g) Tematické centrum mládeže, Nitra
 - h) Tematické centrum mládeže, Trenčín
 - i) Tematické centrum mládeže, Trnava

IV. CENA ZA DIELO A PLATOBNÉ PODMIENKY

1. Cena celkom za dielo je stanovená dohodou v zmysle zákona NR SR č. 18/1996Z.z. o cenách v znení neskorších predpisov ako maximálna, a to vo výške 18.330 eur bez DPH (slovom osemnásťtisícotridsať EUR bez DPH). Celková cena za dielo vrátane DPH 20 % je 21.996 Eur (slovom EUR). Cena je stanovená ako maximálna, vrátane všetkých nákladov zhotoviteľa.
2. Zhotoviteľ bude objednávateľovi fakturovať dohodnutú cenu diela až po riadnom ukončení a odovzdaní diela, po jednotlivých celkoch, ktoré budú odovzdávané podľa preberacích protokolov, potvrdených zástupcami zmluvných strán.
3. Faktúra musí obsahovať okrem náležitostí daňového dokladu aj špecifikáciu fakturovanej ceny.
4. Lehota splatnosti faktúry je 14 dní odo dňa jej riadneho doručenia objednávateľovi. Faktúra bude uhrádzaná výhradne prevodným príkazom.
5. Faktúru je nevyhnutné zasielať doporučené v obálke označenej slovom „Faktúra“ na adresu: IUVENTA, Karloveská 64, 842 58 Bratislava 4. Pri faktúrach, ktoré nie sú doručované osobne alebo doporučené poštou nemožno vymáhať úrok z omeškania podľa Článku V. bod 1. tejto zmluvy.
6. Za správne vyčíslenie výšky dane z pridanej hodnoty podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov zodpovedá v plnom rozsahu zhotoviteľ.
7. V prípade, že faktúra nebude obsahovať náležitosti uvedené v tejto zmluve, objednávateľ je oprávnený vrátiť faktúru zhotoviteľovi na doplnenie faktúry s uvedením nedostatkov, ktoré sa majú odstrániť. V tomto prípade sa preruší plynutie lehoty splatnosti a nová lehota splatnosti začne plynúť dňom riadneho doručenia opravenej faktúry objednávateľovi.

8. Právo na zaplataenie dohodnutej ceny diela vzniká zhotoviteľovi riadnym a včasným splnením jeho záväzku.
9. Objednávateľ vyhlasuje, že je platcom DPH. Zhotoviteľ vyhlasuje, že je platcom DPH.

V. ÚROK Z OMEŠKANIA, ZMLUVNÉ POKUTY

1. Ak zhotoviteľ poruší svoj záväzok tým, že riadne a v dohodnutom termíne nevypracuje a neodovzdá objednávateľovi dielo, je objednávateľ oprávnený uplatniť si zmluvnú pokutu vo výške 5% z celkovej ceny diela dohodnutej touto zmluvou. Zaplatením zmluvnej pokuty nie je dotknutý nárok objednávateľ na náhradu škody.
2. Zmluvnú pokutu, ktorá sa viaže k porušeniu záväzku odovzdania diela zhotoviteľom v dohodnutom termíne objednávateľ neuplatní, pokiaľ takémuto porušeniu záväzku budú predchádzať skutočnosti uvedené podľa ustanovení v kapitole VII. 1.1 tejto zmluvy.
3. Ak objednávateľ neuhradí cenu diela po jeho riadnom zhotovení a odovzdaní v lehote splatnosti podľa čl. IV. Bod 4. tejto zmluvy, má zhotoviteľ právo uplatniť úrok z omeškania z fakturovanej ceny diela vo výške ustanovenej v § 1 ods. 1 Nariadenia vlády SR č.21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka.

VI. LICENCIA

1. Zhotoviteľ vyhlasuje, že je oprávnený vykonávať vo svojom mene a na svoj účet majetkové práva k softvéru ISSR, ktoré je predmetom tejto zmluvy.
2. Zhotoviteľ udeľuje objednávateľovi súhlas s používaním softvérovej aplikácie na správu bezpečnostnej dokumentácie (ISSR) v súvislosti s výkonom jeho činnosti a to odo dňa podpisu preberacieho protokolu.
3. Zhotoviteľ udeľuje objednávateľovi licenciu v neobmedzenom rozsahu a na neurčitý čas. V súvislosti so zhotovením diela dodá zhotoviteľ pre objednávateľa 1 serverovú licenciu a 1 kus užívateľských licencií.
4. V súvislosti s postúpením licencie zabezpečí zhotoviteľ všetky súvisiace právne vzťahy podľa autorského zákona.

VII. ZÁVÄZKY ZMLUVNÝCH STRÁN

1. Objednávateľ sa zaväzuje:
 - 1.1. 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.
 - 1.2. Oznámiť zhotoviteľovi zrušenie plánovaného pracovného stretnutia najneskôr 1 deň pred týmto plánovaným pracovným stretnutím.
 - 1.3. Brať na vedomie, akceptovať a riešiť oprávnené pripomienky zhotoviteľa o zistených skutočnostiach, ktoré by mohli výrazne ovplyvniť alebo ohroziť splnenie predmetu zmluvy.
 - 1.4. Umožniť zamestnancom zhotoviteľa prístup do všetkých priestorov, k zariadeniam a požadovaným podkladom súvisiacim s predmetom zmluvy.
 - 1.5. 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:
 - 2.1. Plniť a splniť predmet tejto zmluvy s odbornou starostlivosťou a v zmysle príslušných ustanovení zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení, vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení,

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 MF SR v rozsahu diela.

- 2.2. 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.
- 2.3. Dodržiavať termíny dohodnutých pracovných stretnutí medzi zhotoviteľom a objednávateľom.
- 2.4. Oznámiť objednávateľovi zrušenie plánovaného pracovného stretnutia najneskôr 1 deň pred týmto plánovaným pracovným stretnutím.
- 2.5. Chrániť vlastnícke práva objednávateľa a zachovávať dôvernosť pri priamych alebo sprostredkovaných informáciách, 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 vzniknutej škody na zhotoviteľovi, na základe preukázania vzniku škody a výšky vzniknutej škody znaleckým posudkom.
- 2.6. Informovať objednávateľa o zistených skutočnostiach, ktoré by mohli výrazne ovplyvniť alebo ohroziť splnenie predmetu tejto zmluvy.
- 2.7. Bezodkladne po podpise tejto zmluvy písomne oznámiť objednávateľovi zoznam pracovníkov zhotoviteľa, ktorí sa budú podieľať na zhotovení diela s uvedením mena, priezviska, bydliska, dátumu narodenia, resp. čísla preukazu totožnosti

VIII. ZÁRUKA, ZODPOVEDNOSŤ ZA VADY

1. Zhotoviteľ poskytuje na predmet zmluvy záruku 24 mesiacov od jeho protokolárneho prevzatia objednávateľom. Za odstránenie zistených väd v odovzdanej 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.

IX. ODSŤÚPENIE OD ZMLUVY

1. Zmluvné strany sa dohodli, že od zmluvy môžu odstúpiť pri podstatnom porušení zmluvných dojednaní v týchto prípadoch:
 - 1.1. 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 po dobu dlhšiu ako 30 kalendárnych dní po zmluvne dohodnutom termíne uvedenom v čl. III. bod 1. tejto zmluvy a v prípade porušenia záväzkov zhotoviteľa uvedených v čl. VII. bod 2 tejto zmluvy.
 - 1.2. Zhotoviteľ je oprávnený odstúpiť od zmluvy v prípade, že objednávateľ je v omeškaní s úhradou dohodnutej ceny diela dlhšie ako 30 kalendárnych dní po lehote splatnosti riadne 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.

X. 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 zverejnením v plnom rozsahu.
2. Túto zmluvu možno zmeniť alebo dopĺňať 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 3 rovnopisoch, z ktorých 2 rovnopisy obdrží objednávatel' a 1 rovnopis obdrží zhotoviteľ.
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 či neúčinného. Do uzavretia takého dodatku platí zodpovedajúca právna úprava všeobecne záväzných právných predpisov Slovenskej republiky.
7. Na vecné konanie v rozsahu tejto zmluvy splnomocňuje:
Zhotoviteľ:
Objednávatel': Vladimír Kollár, tel: 02/ 592 96 202 mail: vladimir.kollar@iuventa.sk
8. Neoddeliteľnou súčasťou zmluvy je:
Príloha č. 1 - Obsahová špecifikácia predmetu zmluvy.
Príloha č. 2 – Výpis z obchodného registra zhotoviteľa (nie starší ako 2 týždne).
9. Zmluvné strany prehlasujú, že si zmluvu prečítali, jej obsahu a právnym účinkom z nej vyplývajúcich porozumeli, zmluva nebola uzavretá v tiesni ani za jednostranné nevýhodných podmienok a na znak súhlasu s jej znením ju vlastnoručne oprávnenými zástupcami zmluvných strán podpísali.

V Bratislave, dňa :

V Trenčianskych Tepliciach dňa :

Za objednávateľa

Za zhotoviteľa

.....
Ing. Viliam Michalovič
Generálny riaditeľ

.....
Roman Václav
konateľ Datasoft Consulting s.r.o.

Príloha č.1 (Vychádza zo súťažného návrhu)

1. kompletná ochrana osobných údajov :

BEZPEČNOSTNÁ DOKUMENTÁCIA – BEZPEČNOSTNÝ PROJEKT v rozsahu :

- 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. 122/2013 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. 122/2013 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 detailizáciu 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 kópií 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, prijaté 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, prijaté 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.

Príloha č. 1 zoznam a vzor dotazníkov analytickej časti

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 so 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 OÚ.
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 č.122/2013 Z.z na ochranu OÚ.
12. **Zoznam dôležitých procesov súvisiacich so spracúvaním OÚ.** – Obsahuje zoznam a popis jednotlivých procesov súvisiacich so spracúvaním OÚ (Proces získavania OÚ, Proces likvidácie OÚ,)

Predpokladaná časová lehota :

záleží od súčinnosti oprávnených osôb prevádzkovateľa. Predpokladaná lehota plnenia je 15 pracovných dní (osobodní)

2. **Pravidlá bezpečnosti informačných systémov, 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. 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 pozícií 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 sietí 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 do 10 pracovných dní (osobodní)

Voliteľné doplnkové riešenie nad rámec ponuky :

- realizácia prienikového testovania za účelom zistenia slabých miest prevádzkovateľa. Rozsah prác max. 10 osobodní.

3. Preškolenia oprávnených osôb a špecialistov IKT

Školenie pre poverené oprávnené osoby :

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

Rozsah školenia k ochrane osobných údajov:

- b) 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.
- c) Definície základných pojmov ochrany OÚ, povinnosti prevádzkovateľa, povinnosti zodpovednej osoby, atď
- d) Bezpečnostný projekt a smernice na ochranu osobných údajov v rozsahu :
3a, informačné systémy, v ktorých organizácia 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
- e) Práva dotknutých osôb.
- f) Požiadavky na systém ochrany OÚ (bezpečnostné smernice, bezpečnostný projekt, ochranné opatrenia)
- g) Úrad na ochranu OÚ – postavenie, kontrolná a metodická činnosť
- h) Informačná bezpečnosť v systéme riadenia ochrany osobných údajov
- i) Nástroje na automatizovanú správu dokumentácie zjednodušujúce dohľad nad ochranou OÚ u prevádzkovateľa

Rozsah školenia k informačnej bezpečnosti, 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 technológií.
- §42 účasť tretej strany.

5. Metodiky analýzy rizík

6. Interné audit 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.

4. Softvérová podpora pre riadenie, správu a dohľad nad komplexným systémom ochrany osobných údajov a informačnej bezpečnosti , vrátane automatizovanej správy bezpečnostnej dokumentácie :

- 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 IUVENTU ako autor aplikácie poskytneme na časovo neobmedzené používanie licencie v počte : 1 serverová licencia + 1 užívateľskú licenciu. Optimálny stav je vtedy, ak počet užívateľských licencií je rovnaký ako počet oprávnených osôb.

Aplikácia ISSR garantuje riadený prístup užívateľov k jednotlivým modulom aplikácie.

ISSR - moduly

Aplikácia ISSR bude pre IUVENTU 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. 122/2013 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 environment, 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 IUVENTU :

- bezplatná podpora a aktualizácia počas 12 mesiacov od implementácie.
- voliteľná platená podpora a aktualizácia vo výške max. 15% obstarávacích nákladov / ročne po uplynutí bezplatnej podpory

5. Implementácia v organizácii a naplnenie dát do softvérovej aplikácie ISSR

Implementácia aplikácie prebehne v užívateľskom prostredí IUVENTY.

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.

6. Príprava zodpovednej osoby z organizácie na skúšku pred lektorským zborom Úradu na ochranu osobných údajov

Príprava zodpovednej osoby (1 až 4 osoby z IUVENTY) bude spočívať v jednodennom konkretizovanom školení k problematike ochrany osobných údajov podľa nového zákona č. 122/2013 Z.z.

Odovzdanie diela :

A. dielo podľa požiadaviek odovzdávame osobe poverenej štatutárom organizácie. Účastný môže byť štatutár organizácie, resp. ďalšia štatutárom poverená osoba.

Dielo bude odovzdávané po jednotlivých logických celkoch a fakturované na základe preberacích protokolov za jednotlivé celky.

B. Pri odovzdávaní diela postupujeme nasledovným spôsobom :

- podrobne rozoberieme a rozdiskutujeme každú časť Bezpečnostného Projektu a dokumentácie
- súčasťou diskusie je vysvetlenie a komentár každej časti dokumentácie

C. Protokolárne odovzdanie

Podporná činnosť pri účasti na kontrolách inšpekčných orgánov kontrolných osôb (Úrad na ochranu OÚ, Ministerstvo Financíi SR)

V prípade požiadavky na účasť audítora pri kontrole aktuálneho stavu informačných systémov u prevádzkovateľa vykonávanej príslušnými kontrolnými orgánmi, alebo formulácie odpovedí k úradným záznamom a návrhom na nápravu zistených prípadných nedostatkov, sme pripravení poskytnúť podporu v plnom rozsahu, podľa vopred dohodnutých podmienok.

Cena za pravidelné kontroly a revízie bezpečnostnej dokumentácie a stavu riadenia ochrany aktív organizácie

Štandardne vykonávame podporu tak pri kontrole inšpekčných orgánov ako aj pri interných revíziách dokumentácie, interných auditoch, bezpečnostnom poradenstve, na základe dohodnutých zmluvných podmienok. Pokiaľ tieto podmienky nie sú súčasťou realizácie diela, sú účtované individuálne, podľa

rozsahu prác. Navrhovaná zmluvná cena pre rok 2013 je **1 auditohodina = 90 eur s dph vrátane všetkých nákladov v rámci SR.**

Ostatné podmienky, dôvernosť a mlčanlivosť :

V prípade realizácie diela sa ako zhotoviteľ zaväzujeme k nasledovným obmedzeniam :

- chrániť vlastnícke práva odberateľa a zachovávať dôvernosť pri priamych alebo sprostredkovaných informáciach, podkladoch a dokumentácii, ktorú obdržia jeho pracovníci.
- dodržiavať mlčanlivosť o skutočnostiach, o ktorých sa zhotoviteľ dozvedel v súvislosti s plnením predmetu tejto zmluvy.