Zmluva o dielo

č. u objednávateľa: ZML-1-4/2023-500
č. u zhotoviteľa: SK2305/01

Táto zmluva sa uzatvára podľa § 536 a nasl. Obchodného zákonníka v znení neskorších predpisov a § 83 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov medzi:

OBJEDNÁVATEĽOM:

Názov:	Štatistický úrad Slovenskej republiky
Sídlo:	Lamačská cesta 3/C, 840 05 Bratislava, Slovenská republika
Zastúpený:	Ing. Peter Peťko, MBA, predseda úradu
IČO:	00166197
DIČ:	2020830218
Bankové spojenie:	Štátna pokladnica
IBAN:	SK46 8180 0000 0070 0007 2444

(ďalej len „objednávateľ“)

a

ZHOTOVITEĽOM:

Názov:	SOITRON, s.r.o.
Sídlo:	Plynárenská 5, 829 75 Bratislava, Slovenská republika
Zastúpený:	Ing. Marián Skákala, výkonný riaditeľ a konateľ spoločnosti
IČO:	35955678
DIČ:	2022066937
Bankové spojenie:	Tatra Banka a.s.
IBAN:	SK40 1100 0000 0026 2583 2658

(ďalej len „zhotoviteľ“)

(objednávateľ a zhotoviteľ súčasne ako „zmluvné strany“)

PREAMBULA

A. Zmluva je uzatvorená ako výsledok verejného obstarávania zákazky s názvom „**Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS**“, na základe ktorého zhotoviteľ ako uchádzač uspel v súťaži a ktorého objednávateľ vyzval na uzatvorenie zmluvy.

B. Dielo, ktoré sa na základe zmluvy zhotoviteľ zaväzuje vykonať pre objednávateľa, je nevyhnutné na zvýšenie informačnej bezpečnosti a kybernetickej bezpečností v IKT prostredí objednávateľa.

C. Predmet tejto Zmluvy o dielo bude zo strany objednávateľa financovaný z Operačného programu Integrovaná infraštruktúra („OPII“)

Článok 1
Vymedzenie niektorých pojmov

1.1. Zmluvné strany sa dohodli a súhlasia, že pojmy uvedené nižšie v úvodzovkách majú nasledovný význam:

i. „kľúčový expert“ je fyzická osoba označená zhotoviteľom, prostredníctvom ktorej zhotoviteľ preukazoval splnenie podmienok účasti ako uchádzač v súťaži a ktorá je uvedená v prílohe č. 4, resp. fyzická osoba v súlade s článkom 5;

ii. „nariadenie o európskej štatistike“ je nariadenie Európskeho parlamentu a Rady (ES) č. 223/2009 z 11. marca 2009 o európskej štatistike a o zrušení nariadenia (ES, Euratom) č. 1101/2008 o prenose dôverných štatistických údajov Štatistickému úradu Európskych spoločenstiev, nariadenia Rady (ES) č. 322/97 o štatistike Spoločenstva a rozhodnutia Rady 89/382/EHS, Euratom o založení Výboru pre štatistické programy Európskych spoločenstiev v platnom znení;

iii. „Obchodný zákonník“ je zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov;

iv. „objednávateľ“ je verejný obstarávateľ uvedený v záhlaví tejto zmluvy;

v. „subdodávateľ“ je hospodársky subjekt, ktorý uzavrie alebo uzavrel so zhotoviteľom písomnú odplatnú zmluvu na plnenie určitej časti predmetu tejto zmluvy (zmluvu o subdodávke);

vi. „vyhláška ITVS“ je vyhláška č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológii verejnej správy (ktorou sa zrušil výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov);

vii. „zákon o KB“ je zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;

viii. „zákon o ITVS“ je zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;

ix. „zákon o RPVS“ je zákon č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;

x. „zákon o štátnej štatistike“ je zákon č. 540/2001 Z. z. o štátnej štatistike v znení neskorších predpisov;

xi. „zhotoviteľ“ je zhotoviteľ diela uvedený v záhlaví tejto zmluvy;
xii. „zmluva“ je táto Zmluva o dielo;
xiii. „ZVO“ je zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;

1.2. Význam pojmov podľa bodu 1.1. pri použití množného čísla zostáva zachovaný.

Článok 2
Predmet zmluvy

2.1. Predmetom zmluvy sú záväzky zhotoviteľa:
i. nasadenie bezpečnostných riešení:
- na ochranu auditných záznamov - LOG manager,
- na ochranu citlivých údajov formou DLP (Data Leakage Prevention),
- na riadenie privilegovaných identít a prístupu k heslám privilegovaných účtov PIM (Privileged Identity Management),

ii. vykonať posúdenie bezpečnosti prostredia objednávateľa formou penetračného testovania

(ďalej spolu ako „dielo“).

2.2. Podrobná špecifikácia predmetu zmluvy je uvedená v prílohe č. 1 a v prílohe č. 2.

2.3. Objednávateľ sa zaväzuje za vykonané dielo zaplatiť zhotoviteľovi cenu podľa článku 4.

Článok 3
Čas, miesto a spôsob plnenia zmluvy

3.1. Zhotoviteľ je povinný vykonať dielo:
i. podľa bodu 2.1. písm. ii. do troch (3) mesiacov odo dňa nadobudnutia účinnosti zmluvy,
ii. podľa bodu 2.1. písm. i. najskôr po dni vykonania časti diela podľa bodu 2.1. písm. ii., najneskôr však do 30.09.2023.

3.2. Zhotoviteľ vykoná dielo v sídle objednávateľa a ak to bude nevyhnutné pre riadne plnenie zmluvy v priestoroch zhotoviteľa alebo v iných priestoroch podľa požiadaviek objednávateľa. Pre odstránenie pochybností sa za hlavné miesto plnenia rozumie sídlo objednávateľa. Objednávateľ vytvorí vo svojich priestoroch na vlastné náklady podmienky pre riadne vykonania diela zhotoviteľom. Ak objednávateľ po konzultácii so zhotoviteľom neurčí inak, platí, že zhotoviteľ vykoná dielo v priestore organizovanom a vybavenom objednávateľom ako dátová miestnosť.

3.3. Zhotoviteľ je povinný vykonať dielo alebo jeho časť podľa zmluvy riadne, v súlade so zmluvou a prílohami č. 1 a č. 2, a včas v súlade s lehotami uvedenými v bode 3.1.

3.4. Zhotoviteľ nezodpovedá za nesplnenie svojich povinností podľa zmluvy v prípade, ak nesplnenie bude spôsobené v dôsledku porušení povinností objednávateľa.

3.5. Zhotoviteľ sa zaväzuje pri odovzdaní jednotlivých častí diela podľa bodu 2.1. písm. i. a písm. ii. odovzdať objednávateľovi v elektronickej podobe na dátovom nosiči, v prípade požiadavky objednávateľa aj v listinnej podobe, všetky originály vytvorených výstupov.

3.6. Riadne odovzdanie príslušnej časti diela podľa bodu 2.1. písm. i. a písm. ii. potvrdia zmluvné strany podpísaním preberacieho protokolu.

3.7. Preberací protokol bude obsahovať označenie čiastkových plnení zmluvy, vrátane výkazov prác kľúčových expertov obsahujúcich jednoznačnú identifikáciu kľúčových expertov a rozsah prác, ktoré kľúčový expert vykonal, a dátum podpisu preberacieho protokolu. Preberací protokol bude vyhotovený v dvoch (2) rovnopisoch, z ktorého objednávateľ dostane jeden (1) rovnopis a zhotoviteľ dostane jeden (1) rovnopis.

3.8. Objednávateľ do desiatich (10) pracovných dní odo dňa predloženia návrhu preberacieho protokolu oznámi zhotoviteľovi pripomienky k vykonanému dielu alebo jeho časti. Objednávateľ nie je povinný podpísať preberací protokol, ak vykonané dielo alebo jeho časť nezodpovedajú opisu predmetu zmluvy alebo pokynom objednávateľa. Zhotoviteľ je povinný vykonané dielo alebo jeho časť upraviť v súlade s pripomienkami objednávateľa alebo bez zbytočného odkladu písomne zdôvodniť bezdôvodnosť pripomienok objednávateľa. Objednávateľ najneskôr do desiatich (10) pracovných dní odo dňa predloženia návrhu nového preberacieho protokolu oznámi zhotoviteľovi pripomienky k novému preberaciemu protokolu.

3.9. Ak vykonané dielo alebo jeho časť zodpovedajú opisu predmetu zmluvy alebo pokynom objednávateľa a objednávateľ odmietne podpísať preberací protokol, vykonané dielo alebo jeho časť sa považujú za prevzaté dňom nasledujúcim po dni, ktorým uplynula lehota na zaslanie pripomienok k návrhu preberaciemu protokolu; to rovnako platí aj v prípade, ak objednávateľ uplatnil pripomienky k návrhu nového preberacieho protokolu podľa bodu 3.8.

Článok 4
Cena a platobné podmienky

4.1. Celková cena za dielo je stanovená dohodou zmluvných strán v súlade so zákonom č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhláškou Ministerstva financií Slovenskej republiky č. 87/1996 Z. z. v znení neskorších predpisov, ktorou sa vykonáva zákon č. 18/1996 Z. z. o cenách v znení neskorších predpisov.

4.2. Celková cena za vykonanie diela podľa bodu 2.1. zmluvy je 340 900,00 EUR bez DPH (slovom: tristoštyridsaťtisíc deväťsto eur bez DPH), 409 080,00 EUR s DPH (slovom: štyristodeväťtisíc osemdesiat eur s DPH).

4.3. Záväzný štruktúrovaný rozpočet ceny je uvedený v prílohe č. 5.

4.4. Právo na zaplatenie ceny vznikne zhotoviteľovi na základe faktúry vystavenej po vykonaní príslušnej časti diela podľa bodu 2.1. písm. i. a písm. ii.

4.5. Faktúra je splatná tridsiaty (30.) deň po jej doručení objednávateľovi. Fakturovaná cena je zaplatená dňom, keď sa uhrádzaná čiastka odpíše z účtu objednávateľa.

4.6. Faktúra musí obsahovať náležitosti v zmysle zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v platnom znení. Súčasťou každej faktúry bude podpísaný preberací protokol podľa článku 3. V prípade, že faktúra nebude obsahovať predpísané náležitosti alebo náležitosti uvedené v zmluve, resp. budú v nej uvedené nesprávne, alebo neúplné údaje, je objednávateľ oprávnený túto faktúru vrátiť pred jej splatnosťou. Opravenej faktúre alebo novej faktúre plynie nová tridsať (30) dňová lehota splatnosti od jej doručenia objednávateľovi. Zmluvné strany vyhlasujú, že dojednanie tridsať (30) dňovej lehoty na plnenie podľa predchádzajúcich odsekov nie je v hrubom nepomere k právam a povinnostiam vyplývajúcim zo záväzkového vzťahu pre zhotoviteľa.

4.7. V prípade omeškania zaplatenia faktúry si zhotoviteľ nebude uplatňovať nárok na úrok z omeškania, ak omeškanie bude spôsobené peňažným ústavom objednávateľa.

Článok 5
Práva a povinnosti zmluvných strán

5.1. Zhotoviteľ je povinný pri vykonávaní diela postupovať na vysokej profesionálnej úrovni, so všetkou odbornou starostlivosťou a v súlade so záujmami objednávateľa, ktoré pozná alebo pri vynaložení odbornej starostlivosti musí poznať, a zabezpečiť si všetky dostupné informácie týkajúce sa predmetu zmluvy. Zhotoviteľ sa zaväzuje dodržiavať pri plnení zmluvy všetky právne predpisy, ktoré sú potrebné pre riadne a včasné plnenie zmluvy.

5.2. Objednávateľ sa zaväzuje vydávať pokyny v súlade s platnými a účinnými právnymi predpismi a pred vykonaním diela vhodným spôsobom a v miere nevyhnutnej pre riadne a včasné plnenie zmluvy oboznámiť alebo zabezpečiť oboznámenie zhotoviteľa s právnymi predpismi a inými záväznými dokumentmi vydanými príslušnými orgánmi verejnej moci v Slovenskej republike a orgánov Európskej únie vzťahujúcimi sa na vykonanie diela.

5.3. Zhotoviteľ je povinný plniť riadne a včas svoje povinnosti podľa zmluvy a dodržiavať pokyny objednávateľa. Zhotoviteľ je povinný upozorniť objednávateľa bez zbytočného odkladu na nevhodnú povahu pokynov alebo na ich rozpor s ustanoveniami zmluvy a/alebo ustanoveniami právnych predpisov, ak zhotoviteľ mohol túto nevhodnosť alebo rozpor zistiť pri vynaložení všetkej odbornej starostlivosti. Ak nevhodné alebo so zmluvou a/alebo právnymi predpismi rozporné pokyny prekáža v riadnom plnení zmluvy, je zhotoviteľ povinný jej splnenie v nevyhnutnom rozsahu prerušiť do doby zmeny predmetného pokynu alebo písomného oznámenia, že objednávateľ trvá na plnení zmluvy podľa daných pokynov. O dobu, po ktorú bolo potrebné prerušiť plnenie zmluvy, sa predlžuje lehota určená na jej splnenie.

5.4. Zhotoviteľ, ktorý splnil povinnosť uvedenú v bode 5.3., nezodpovedá za nemožnosť splnenia zmluvy alebo za vady vykonaného diela spôsobené pokynmi, ktoré sú nevhodné alebo sú v rozpore s právnymi predpismi, ak objednávateľ na nich pri plnení zmluvy písomne trval.

5.5. Zhotoviteľ, ktorý nesplnil povinnosť uvedenú v bode 5.3., zodpovedá za vady plnenia zmluvy spôsobené nevhodnými alebo so zmluvou a/alebo všeobecne záväznými právnymi predpismi rozpornými pokynmi.

5.6. Zhotoviteľ je povinný zabezpečiť, aby sa kľúčoví experti, priamo podieľali na plnení zmluvy. Tým nie je dotknuté právo zhotoviteľa realizovať predmet zmluvy aj prostredníctvom iných expertov, avšak kľúčové úlohy pri plnení zmluvy musia zastávať kľúčoví experti.

5.7. Po predchádzajúcom písomnom súhlase objednávateľa a iba na základe vyhotovenia dodatku k tejto zmluve môže zhotoviteľ na vykonanie predmetu zmluvy použiť iných kľúčových expertov než kľúčových expertov uvedených v prílohe č. 4, ktorí spĺňajú požiadavky, ktoré boli kladené na daného kľúčového experta vo verejnom obstarávaní, pričom taká zmena nebude mať za následok navýšenie ceny diela podľa článku 4.

5.8. Za účelom zmeny v osobe kľúčového experta je zhotoviteľ povinný doručiť objednávateľovi žiadosť o zmenu v prílohe č. 4, ktorá musí obsahovať identifikačné

údaje navrhovaného kľúčového experta, ktorý by mal zastávať kľúčové úlohy pri vykonávaní predmetu zmluvy alebo jeho časti alebo iného plnenia podľa zmluvy.

5.9. Zhotoviteľ je povinný priložiť k žiadosti podľa bodu 5.8. doklady preukazujúce splnenie podmienok podľa bodu 5.7., nové znenie prílohy č. 4 a návrh dodatku tejto zmluvy, týkajúci sa zmeny kľúčového experta.

5.10. Každá žiadosť podľa bodu 5.8., vrátane súvisiacich dokumentov podľa bodu 5.8., musí byť objednávateľovi odovzdaná včas tak, aby nezdržiavala postup vykonávania diela. Objednávateľ je povinný vyjadriť sa k žiadosti, obsahujúcej všetky požadované údaje navrhovaného kľúčového experta podľa bodu 5.8. a všetky požadované dokumenty podľa bodu 5.8., s uvedením, či so zmenou súhlasí alebo nie najneskôr do troch (3) pracovných dní odo dňa jej doručenia, v opačnom prípade sa predpokladá, že s navrhovanou zmenou zoznamu kľúčových expertov súhlasí.

5.11. Zmluvné strany vyhlasujú, že odsúhlasenie zmeny kľúčových expertov zo strany objednávateľa a tomu zodpovedajúce vyhotovenia a podpis dodatku k zmluve žiadnym spôsobom nezbavuje zhotoviteľa záväzkov vyplývajúcich mu zo zmluvy a že také zmeny nesmú mať za následok navýšenie ceny diela podľa článku 4.

5.12. Objednávateľ je povinný poskytnúť zhotoviteľovi potrebnú súčinnosť pri plnení zmluvy, najmä poskytnúť zhotoviteľovi všetky podklady, ktoré sú nevyhnutné pre vykonanie diela alebo jeho časti. Objednávateľ zodpovedá za správnosť a úplnosť ním poskytnutých podkladov.

5.13. Zhotoviteľ sa zaväzuje bezodkladne písomne informovať objednávateľa o každom prípadnom zdržaní, či iných skutočnostiach, ktoré by mohli ohroziť včasné a riadne plnenie zmluvy.

5.14. V prípade, že sa vyskytne udalosť, ktorá jednej alebo obom zmluvným stranám neumožní plnenie ich zmluvných povinností, sú povinné sa o tom bez zbytočného odkladu informovať a navrhnúť druhej zmluvnej strane spôsob riešenia následkov udalosti. Nesplnenie tejto povinnosti zakladá nárok na náhradu škody pre tú zmluvnú stranu, ktorá sa porušenia zmluvy v tomto bode nedopustila.

5.15. Zhotoviteľ sa zaväzuje umožniť oprávneným osobám príslušných orgánov verejnej moci výkon kontroly, auditu alebo dozoru súvisiaceho s vykonaním diela kedykoľvek počas platnosti zmluvy, aj po jej ukončení. Oprávnenými osobami sú osoby poverené napríklad Najvyšším kontrolným úradom Slovenskej republiky, Úradom vládneho auditu na výkon kontroly, auditu, dohľadu alebo dozoru vrátane prizvaných osôb.

5.16. Objednávateľ je oprávnený počas vykonávania diela alebo jeho časti pokynom nariadiť zhotoviteľovi úpravu predmetu diela najmä z dôvodu zmien právnych predpisov iba za predpokladu, že pokyn nemá vplyv na výšku ceny za dielo alebo jeho časť a/alebo nákladov zhotoviteľa spojených s vykonaním diela alebo jeho časti a/alebo rozsah činností potrebných na vykonanie diela alebo jeho časti.

5.17. Zhotoviteľ je povinný pri plnení tejto zmluvy dodržiavať zásady poctivého obchodného styku a zdržať sa akéhokoľvek konania, ktoré by mohlo byť posúdené ako konanie v rozpore s dobrými mravmi hospodárskej súťaže.

5.18. Zhotoviteľ je povinný zdržať sa pri plnení zmluvy akéhokoľvek konania, ktoré by mohlo v dôsledku konfliktu záujmov spochybniť nestrannosť a základný účel plnenia zmluvy. Konfliktom záujmov podľa predchádzajúcej vety je uprednostnenie osobného záujmu zhotoviteľa pred záujmom na riadnom plnení zmluvy, a môže vzniknúť najmä v dôsledku ekonomických záujmov, politických alebo národnostných preferencií, rodinných vzťahov, alebo vzťahov s blízkymi osobami alebo iného spojenia alebo

spoločných záujmov. Zhotoviteľ sa zaväzuje bezodkladne písomne oznámiť objednávateľovi vznik konfliktu záujmov a vykonať kroky na odstránenie akejkoľvek skutočnosti, ktorá by mohla byť považovaná za konflikt záujmov.

5.19. Objednávateľ je oprávnený oznámiť písomne zhotoviteľovi pozastavenie realizácie zmluvy alebo akejkoľvek jej časti na takú dobu a takým spôsobom, ktorý považuje za potrebný.

5.20. Zhotoviteľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu údajov týkajúcich sa bankového účtu zhotoviteľa, na ktorý má objednávateľ posielať platby podľa zmluvy; oznámenia sa nevyžaduje, ak zhotoviteľ uvádza bankový účet, na ktorý má byť zaslaná platba vo faktúre, ktorou si uplatňuje právo na zaplatenie ceny.

5.21. Zhotoviteľ nie je oprávnený bez predchádzajúceho písomného súhlasu objednávateľa postúpiť akékoľvek svoje práva z tejto zmluvy na tretiu osobu.

5.22. Zhotoviteľ musí byť pre každé z ním navrhovaných bezpečnostných riešení uvedených v prílohe č. 2 autorizovaným partnerom výrobcu bezpečnostného riešenia. Zhotoviteľ je povinný kedykoľvek na písomnú výzvu objednávateľa preukázať v lehote troch (3) pracovných dní od doručenia výzvy objednávateľa splnenie povinnosti podľa predchádzajúcej vety. Porušenie povinnosti zhotoviteľa podľa prvej a/alebo druhej vety tohto bodu sa považuje za podstatné porušenie tejto zmluvy.

5.23. Zhotoviteľ je povinný strpieť výkon kontroly, auditu a/alebo kontroly na mieste súvisiacich s vykonávaným dielom alebo jeho častí kedykoľvek počas platnosti a účinnosti Zmluvy o poskytnutí nenávratného finančného príspevku č. Z311071BGP1, z ktorého je financovaná táto zmluva, a to oprávnenými osobami na výkon tejto kontroly, auditu a/alebo kontroly na mieste a poskytnúť týmto osobám všetku potrebnú súčinnosť.

Článok 6
Vady diela a zodpovednosť za vady

6.1. Dielo má vady, ak je vykonané v rozpore so zmluvou, najmä a však nielen v rozpore s požiadavkami uvedenými v prílohe č. 1 a v rozpore s vlastným návrhom plnenia zhotoviteľa uvedenom v prílohe č. 2.

6.2. V prípade, ak má dielo vady podľa bodu 6.1., je zhotoviteľ povinný vady bezplatne odstrániť. Objednávateľ je povinný vadu oznámiť zhotoviteľovi bezodkladne, najneskôr však do piatich (5) pracovných dní po tom, čo takúto vadu diela zistí.

6.3. Zhotoviteľ je povinný začať s odstraňovaním riadne oznámenej vady plnenia do dvadsiatich štyroch (24) hodín odo dňa jej oznámenia.

6.4. Uplatnené vady diela sa zhotoviteľ zaväzuje odstrániť v čo najkratšom možnom termíne, najneskôr do pätnástich (15) dní odo dňa oznámenia zhotoviteľovi. V prípade, ak si povaha a rozsah vady diela vyžaduje dlhšiu lehotu na odstránenie, zhotoviteľ odstráni vady diela v lehote určenej dohodou zmluvných strán. Pokiaľ sa zmluvné strany nedohodnú na lehote pre odstránenie vád diela podľa predchádzajúcej vety, zhotoviteľ je povinný vadu plnenia odstrániť najneskôr do tridsiatich (30) dní odo dňa oznámenia zhotoviteľovi.

6.5. Uplatnené vady diela sa považujú za odstránené dňom podpisu protokolu o odstránení vád diela.

6.6. Zhotoviteľ je zároveň povinný bez zbytočného odkladu nahradiť objednávateľovi alebo tretím osobám škodu, ktorá im vznikla, a to na vlastné náklady.

6.7. Záručná doba na dielo je tridsaťšesť (36) mesiacov odo dňa odovzdania diela ako celku.

Článok 7
Jazyk zmluvy, doručovanie a komunikácia

7.1. Jazyk zmluvy a celej písomnej komunikácie medzi zmluvnými stranami a tretími osobami je slovenský jazyk.

7.2. Zmluvné strany sa zaväzujú vzájomne spolupracovať a poskytovať si všetky informácie potrebné pre riadne plnenie svojich záväzkov pre realizáciu zmluvy. Zmluvné strany sú povinné informovať druhú zmluvnú stranu o všetkých skutočnostiach, ktoré sú alebo môžu byť dôležité pre riadne plnenie zmluvy.

7.3. Každá komunikácia medzi zmluvnými stranami bude prebiehať prostredníctvom oprávnených osôb zmluvných strán, ktorých meno a kontaktné údaje minimálne v rozsahu telefónne číslo a e-mail si zmluvné strany navzájom oznámia do piatich pracovných dní od podpisu tejto zmluvy. Každá zo zmluvných strán môže zmeniť oprávnené osoby. Takáto zmena je účinná dňom doručenia písomného oznámenia o zmene obsahujúceho aj meno a kontaktné údaje novej oprávnenej osoby druhej zmluvnej strane.

7.4. Všetky oznámenia medzi zmluvnými stranami, ktoré sa vzťahujú k zmluve alebo ktoré majú byť vykonané na základe zmluvy, musia byť vykonané v písomnej podobe a druhej zmluvnej strane doručené buď osobne alebo doporučeným listom či inou formou registrovaného poštového styku na adresu uvedenú na titulnej stránke tejto zmluvy, ak nie je ustanovené alebo medzi zmluvnými stranami dohodnuté inak. Písomnú formu považujú zmluvné strany za zachovanú aj v prípade elektronickej komunikácie cez elektronickú poštu alebo cez Ústredný portál verejnej správy.

7.5. Elektronická komunikácia cez elektronickú poštu bude prebiehať zasielaním e-mailov prostredníctvom nasledujúcich adries:

i. adresa objednávateľa: pavol.vadovic@statistics.sk
ii. adresa zhotoviteľa: peter.dzunka@soitron.com

7.6. V prípade pochybností ohľadom času doručenia sa oznámenie považuje za doručené tretím dňom po jeho preukázateľnom odoslaní.

7.7. Doručením sa rozumie prijatie oznámenia zmluvnou stranou, ktorej bola adresovaná.

7.8. Za deň doručenia oznámenia zmluvnej strane, ktorej bolo adresované, sa považuje takisto aj deň,

i. v ktorom ho táto zmluvná strana odoprela prijať,
ii. ktorým márne uplynula odberná lehota pre jeho vyzdvihnutie si na pošte alebo,
iii. v ktorý bola na oznámení zamestnancom pošty vyznačená poznámka, že „adresát sa odsťahoval“, „adresát je neznámy“ alebo iná obdobná poznámka, ktorá podľa poštového poriadku znamená nedoručiteľnosť oznámenia.

Článok 8
Ochrana dôverných informácií

8.1. Všetky informácie obsiahnuté v zmluve, ako i tie, ktoré si zmluvné strany navzájom poskytli pri uzavretí zmluvy a po uzavretí zmluvy, sa považujú za dôverné, ak ich dotknutá strana neoznačí za iné ako dôverné.

8.2. Dôvernými informáciami podľa bodu 8.1. sú najmä:

i. informácie, ktoré sa týkajú zmluvnej strany (najmä informácie o jej činnosti, štruktúre, hospodárskych výsledkoch, všetky zmluvy, finančné, štatistické a účtovné informácie, informácie o jej majetku, aktívach a pasívach, pohľadávkach a záväzkoch, informácie o jej technickom a programovom vybavení, know-how, hodnotiace štúdie a správy, podnikateľské stratégie a plány, informácie týkajúce sa predmetov chránených právom priemyselného alebo iného duševného vlastníctva a všetky ďalšie informácie o zmluvnej strane),

ii. informácie, ktoré sú výslovne zmluvnou stranou označené ako „dôverné“, „confidential“, „proprietary“ alebo iným obdobným označením, a to od okamihu oznámenia tejto skutočnosti druhej zmluvnej strane,

iii. informácie, pre ktoré je stanovený všeobecne záväznými právnymi predpismi Slovenskej republiky osobitný režim nakladania (najmä obchodné tajomstvo, bankové tajomstvo, telekomunikačné tajomstvo, daňové tajomstvo, utajované skutočnosti),

iv. dôverné štatistické údaje podľa § 2 ods. 2 písm. e) zákona o štátnej štatistike a čl. 3 ods. 7 nariadenia o európskej štatistike,

v. osobné údaje, ktoré nie sú dôvernými štatistickými údajmi.

8.3. Ochrana dôverných informácií podľa zmluvy spočíva v záväzku každej zmluvnej strany dodržiavať právne predpisy vzťahujúce sa na ochranu dôverných informácií a pravidlá ochrany dôverných informácií podľa tejto zmluvy.

8.4. Zmluvné strany nakladajú s dôvernou informáciou poskytnutou druhou zmluvnou stranou tak, aby nedošlo k zneužitiu dôvernej informácie alebo hrozbe jej zneužitia s možnosťou porušenia povinnosti, práva alebo právom chráneného záujmu zmluvnej strany alebo inej osoby, a zdržia sa takého konania, ktorého následkom dôjde alebo môže dôjsť k porušeniu povinnosti, práva alebo právom chráneného záujmu zmluvnej strany alebo inej osoby.

8.5. Dôverné informácie okrem dôverných štatistických údajov a/alebo osobných údajov poskytnuté zmluvnou stranou môže druhá zmluvná strana využívať na iné účely ako je plnenie zmluvy, poskytnúť tretej osobe alebo zverejniť ich, len ak zmluvná strana na to dá vopred písomný súhlas a poskytnutie takéhoto súhlasu nie je porušením právnych predpisov.

8.6. Zmluvné strany zabezpečia, aby sa osoby poverené úlohami v rámci plnenia zmluvy preukázateľným spôsobom zaviazali, že zachovajú dôvernosť informácií, ak nie sú viazané vhodnou povinnosťou zachovávať dôvernosť informácií vyplývajúcou z interných predpisov zmluvnej strany alebo z právnych predpisov. Prostriedkom na zachovanie dôvernosti informácií podľa prvej vety je okrem iného aj záväzok mlčanlivosti. Dodržiavanie pravidiel ochrany dôverných informácií vrátane záväzku mlčanlivosti trvá aj po zániku ostatných záväzkov zmluvných strán podľa tejto zmluvy, najdlhšie však do skončenia doby, počas ktorej je informácia dôverná.

8.7. Zmluvné strany sa zaväzujú, že všetky dokumenty, materiály a elektronické nosiče údajov, ktoré obsahujú dôverné informácie, sa budú uchovávať:
   i. osobitne od všetkých ostatných dokumentov, materiálov a poznámok, a to takým spôsobom, aby boli rozpoznateľné ako dôverné informácie,
   ii. na bezpečnom mieste s cieľom ochrániť ich pred odcudzením, neoprávnenou manipuláciou alebo neoprávneným prístupom vrátane zhotovovania kópií údajov.

8.8. Zmluvné strany budú vyhotovovať kópie dôverných informácií len s predchádzajúcim písomným súhlasom druhej zmluvnej strany a v rozsahu nevyhnutnom pre plnenie zmluvy. Zmluvné strany si písomne dohodnú spôsob uchovávania, vyraďovania a likvidovania vyhotovených kópií.

8.9. Zmluvné strany sa zaväzujú vzájomne bezodkladne informovať, ak sa dozvedia o skutočnom alebo hroziacom neoprávnenom použití alebo skutočnom alebo hroziacom neoprávnenom sprístupnení dôverných informácií, a dotknutá strana sa zaväzuje prijať všetky primerané opatrenia s cieľom znemožniť alebo ukončiť akékoľvek takéto použitie alebo akékoľvek takéto sprístupnenie, v prípade potreby za súčinnosti druhej zmluvnej strany.

8.10. Porušením dôvernosti informácií vzniká záväzok zmluvnej strany, ktorá dôvernosť informácie porušila nedodržaním ustanovení tejto zmluvy alebo porušením právnych predpisov, podľa povahy porušenia a povahy dôvernej informácie ukončiť činnosť vedúcu k porušeniu dôvernosti informácií, odstrániť následky porušenia uvedením do pôvodného stavu, prijať opatrenia na zamedzenie porušenia dôvernosti informácií v budúcnosti a preukázať druhej zmluvnej strane ich plnenie, ak zmluvný vzťah naďalej trvá, alebo nahradiť škodu spôsobenú porušením.

8.11. Ohrozením dôvernosti informácií vzniká záväzok zmluvnej strany, ktorá dôvernosť informácie porušila nedodržaním ustanovení tejto zmluvy alebo porušením právnych predpisov, podľa povahy porušenia a povahy dôvernej informácie ukončiť činnosť vedúcu k porušeniu dôvernosti informácií a ak zmluvný vzťah naďalej trvá, prijať opatrenia na zamedzenie ohrozenia alebo porušenia dôvernosti informácií v budúcnosti, a preukázať druhej zmluvnej strane ich plnenie.

8.12. Povinnosť zmluvnej strany poskytnúť dôverné informácie podľa príslušných právnych predpisov nie je zmluvou dotknutá.

8.13. Ustanovenia tohto článku sa primerane vzťahujú aj na dôverné údaje týkajúce sa IKT prostredia objednávateľa, ak nie je v článku 12 uvedené inak.

Článok 9
Sankcie

9.1. Nárok na zaplatenie zmluvných pokút dohodnutých medzi zmluvnými stranami v zmluve vzniká dotknutej zmluvnej strane dňom porušenia zabezpečovanej zmluvnej povinnosti. Pre vznik nároku na zaplatenie zmluvnej pokuty je rozhodné porušenie zabezpečovanej povinnosti. Zavinenie zmluvnej strany sa nevyžaduje.

9.2. Zmluvná strana, ktorá zabezpečenú zmluvnú povinnosť porušila, je povinná príslušnú zmluvnú pokutu zaplatiť druhej zmluvnej strane do tridsiatich (30) dní odo dňa, kedy bola na zaplatenie zmluvnej pokuty vyzvaná druhou zmluvnou stranou.

9.3. Zaplatenie zmluvnej pokuty porušujúcou zmluvnou stranou nezbavuje porušujúcu zmluvnú stranu záväzku splniť povinnosti podľa zmluvy.

9.4. Zmluvná pokuta sa považuje za zaplatenú jej pripísaním na účet zmluvnej strany v peňažnom ústave uvedenom v záhlaví zmluvy.

9.5. Zaplatením zmluvnej pokuty nie je dotknuté právo dotknutej zmluvnej strany na náhradu škody, ktorá jej vznikla porušením povinnosti. Zmluvná pokuta sa nezapočítava na náhradu škody.

9.6. Pre prípad porušenia povinnosti zhotoviteľa vykonať dielo alebo jeho časť riadne a včas, je zhotoviteľ povinný zaplatiť objednávateľovi zmluvnú pokutu vo výške 0,1 % z ceny diela, a to za každý aj začatý deň porušenia zabezpečovanej povinnosti (omeškania), a to za každú zabezpečovanú povinnosť (za každé nedodržanie ktoréhokoľvek termínu) samostatne.

9.7. Pre prípad porušenia povinnosti zhotoviteľa zabezpečiť, aby sa kľúčoví experti priamo podieľali na plnení zmluvy v súlade s bodom 5.6., resp. pre prípad, ak nedôjde k odsúhlasenej zmene ktoréhokoľvek kľúčového experta v súlade s touto zmluvou, je zhotoviteľ povinný zaplatiť objednávateľovi zmluvnú pokutu vo výške 10 % z ceny diela. Pre vylúčenie pochybností sa zmluvné strany dohodli, že zhotoviteľ je povinný zaplatiť objednávateľovi zmluvnú pokutu definovanú v tomto bode zmluvy v prípade, hoci aj len jeden z kľúčových expertov, prostredníctvom ktorých zhotoviteľ ako uchádzač vo verejnom obstarávaní preukazoval splnenie podmienok účasti resp. prostredníctvom odsúhlasených zmenených kľúčových expertov v súlade so zmluvou, sa nebude priamo podieľať na plnení predmetu tejto zmluvy.

9.8. Pre prípad porušenia povinnosti zhotoviteľa uvedenej v bode 5.18. je zhotoviteľ povinný zaplatiť objednávateľovi zmluvnú pokutu vo výške 10 % z ceny diela.

9.9. V prípade omeškania objednávateľa s úhradou faktúry je objednávateľ povinný zaplatiť zhotoviteľovi zákonný úrok z omeškania.

9.10. Pre prípad porušenia povinnosti zhotoviteľa uvedenej v bode 6.3. je zhotoviteľ povinný zaplatiť objednávateľovi zmluvnú pokutu vo výške 500,- EUR (slovom: päťsto eur) za každý aj začatý deň porušenia zabezpečovanej povinnosti, a to za každú zabezpečovanú povinnosť samostatne.

9.11. Pre prípad porušenia povinností zhotoviteľa uvedených v bode 6.4. je zhotoviteľ povinný zaplatiť objednávateľovi zmluvnú pokutu vo výške 500,- EUR (slovom: päťsto eur) za každý aj začatý deň porušenia zabezpečovanej povinnosti, a to za každú zabezpečovanú povinnosť samostatne.

9.12. Pre prípad porušenia akejkoľvek povinnosti zhotoviteľa uvedenej v článku 8 je zhotoviteľ povinný zaplatiť objednávateľovi zmluvnú pokutu vo výške 10 % z ceny diela za každú zabezpečovanú povinnosť samostatne.

9.13. Pre prípad porušenia akejkoľvek povinnosti zhotoviteľa uvedenej v článku 12 je zhotoviteľ povinný zaplatiť objednávateľovi zmluvnú pokutu vo výške 10 % z ceny diela za každú zabezpečovanú povinnosť samostatne.

9.14. Za omeškanie sa nepovažuje stav, ktorý vznikol v dôsledku vyššej moci. O vzniku a trvaní vyššej moci je však dotknutá zmluvná strana povinná druhú zmluvnú stranu bezodkladne písomne informovať.

9.15. Zmluvné strany vyhlasujú, že výška zmluvných pokút dojednaných podľa zmluvy je obvyklá a primeraná povahe a významu zabezpečovaných záväzkov a s touto výškou bez námietok súhlasia.

Článok 10
Poistenie

10.1. Zhotoviteľ je povinný mať najneskôr do desiatich (10) pracovných dní od nadobudnutia účinnosti zmluvy uzatvorené poistenie všeobecnej zodpovednosti za škodu s minimálnou poistnou sumou vo výške 50 % ceny diela podľa bodu 4.2. Poistením musia byť kryté nároky všeobecnej zodpovednosti za škodu na veciach a na zdraví, vrátane ušlého zisku, spôsobené pri vykonávaní diela spôsobenej objednávateľovi alebo tretím osobám.

10.2. Zhotoviteľ je povinný kedykoľvek na písomnú výzvu objednávateľa preukázať v lehote troch (3) pracovných dní od doručenia výzvy objednávateľa splnenie povinnosti podľa bodu 10.1. Poistnú zmluvu v zmysle bodu 10.1. je zhotoviteľ povinný udržať v platnosti a do dňa skončenia záručnej doby na dielo ako celok.

10.3. Porušenie povinnosti zhotoviteľa podľa bodu 10.1. a/alebo 10.2. zmluvy sa považuje za podstatné porušenie tejto zmluvy.

Článok 11
Subdodávatelia

11.1. Na vykonanie diela má zhotoviteľ za podmienok dohodnutých v tejto zmluve právo uzatvárať subdodávateľské zmluvy. Tým nie je dotknutá zodpovednosť zhotoviteľa za plnenie zmluvy v súlade s § 41 ods. 8 ZVO a zhotoviteľ je povinný vykonať dielo sám, na svoju zodpovednosť, v dohodnutom čase a v dohodnutej kvalite.

11.2. Zoznam subdodávateľov s ich identifikačnými údajmi v rozsahu: (i) meno a priezvisko alebo obchodné meno, resp. názov, (ii) adresa pobytu alebo sídlo, (iii) IČO alebo dátum narodenia, ak nebolo pridelené IČO, (iv) podiel plnenia zo zmluvy v percentuálnom vyjadrení, (v) údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia, je uvedený v prílohe č. 3.

11.3. Zhotoviteľ je povinný oznámiť objednávateľovi akúkoľvek zmenu údajov u subdodávateľov a to bezodkladne po tom, ako sa o tejto skutočnosti dozvie.

11.4. V prípade zmeny subdodávateľa je zhotoviteľ povinný najneskôr do piatich (5) pracovných dní odo dňa zmeny subdodávateľa predložiť objednávateľovi informácie o novom subdodávateľovi v rozsahu údajov podľa bodu 11.2., pričom pri výbere subdodávateľa musí zhotoviteľ postupovať tak, aby vynaložené náklady na vykonanie diela na základe zmluvy o subdodávke boli primerané jeho kvalite a cene.

11.5. Zhotoviteľ vyhlasuje, že v čase uzatvorenia tejto zmluvy je zapísaný v registri partnerov verejného sektora v súlade so zákonom o RPVS. Ak sa na strane zhotoviteľa ako zmluvnej strany podieľa skupina dodávateľov podľa § 37 ZVO, má každý člen tejto skupiny dodávateľov povinnosť byť zapísaný v registri partnerov verejného sektora.

11.6. Subdodávateľ alebo subdodávateľ podľa osobitného predpisu, ktorý podľa § 11 ods. 1 ZVO má povinnosť zapisovať sa do registra partnerov verejného sektora, musí byť zapísaný v registri partnerov verejného sektora.

11.7. Povinnosti zhotoviteľa vrátane pravidiel výberu subdodávateľa platia aj pri zmene subdodávateľa počas celej doby trvania tejto zmluvy.

11.8. Zhotoviteľ zodpovedá za plnenie zmluvy o subdodávke subdodávateľa tak, ako keby plnenie realizované na základe takejto zmluvy realizoval sám. Zhotoviteľ zodpovedá za odbornú starostlivosť pri výbere subdodávateľa, ako aj za výsledok plnenia vykonaného na základe zmluvy o subdodávke.

Článok 12
Záväzok informačnej bezpečnosti

12.1. Zhotoviteľ vyjadruje súhlas a v súvislosti s vykonaním diela sa zaväzuje dodržiavať bezpečnostnú politiku objednávateľa, vrátane všeobecných podmienok, ktoré sú uvedené v prílohe č. 6, ďalšie objednávateľom vydané bezpečnostné smernice a štandardy, bezpečnostný projekt objednávateľa, požiadavky na bezpečnosť definované zákonom o KB, zákonom o ITVS a vyhláškou ITVS, a bezpečnostné požiadavky uvedené v tejto zmluve. V prípade výslovného rozporu ustanovení všeobecných podmienok, ktoré sú uvedené v prílohe č. 6 s ustanoveniami tejto zmluvy a nemožnosti ich súčasnej aplikácie majú prednosť ustanovenia tejto zmluvy.

12.2. V prípade, ak objednávateľ vydá alebo zmení bezpečnostné politiky alebo bezpečnostné opatrenia, zhotoviteľ sa zaväzuje oboznámiť sa s nimi bezodkladne po ich prijatí a dodržiavať ich.

12.3. Zhotoviteľ je povinný viesť zoznam svojich pracovných rolí, ktoré majú mať v zmysle tejto zmluvy prístup k informáciám a údajom objednávateľa, pričom je povinný bezodkladne oznámiť objednávateľovi každú zmenu v personálnom obsadení, dotýkajúcu sa výkonu činností v zmysle tejto zmluvy. Zhotoviteľ poskytne objednávateľovi tento zoznam pracovných rolí bezodkladne po uzatvorení tejto zmluvy, alebo aj kedykoľvek na požiadanie objednávateľa.

12.4. Zhotoviteľ je povinný zabezpečiť, že všetky oprávnené osoby, pracovníci zhotoviteľa, ktorí budú vykonávať pre objednávateľa dielo a ktorí budú mať prístup k dôverným informáciám a iným chráneným informáciám a údajom objednávateľa budú zhotoviteľom zaviazaní a podpíšu vyjadrenie o zachovávaní mlčanlivosti a povinnosti dodržiavať bezpečnostné opatrenia (ďalej len „poučené osoby“).

12.5. Zhotoviteľ vytvorí záznam, ktorý bude podpísaný každou z poučených osôb a osobou, ktorá poučenie vykonala. Za riadne poučenie zodpovedá zhotoviteľ. Zhotoviteľ je povinný predložiť objednávateľovi potvrdenie o oboznámení zamestnancov a subdodávateľov s bezpečnostnými požiadavkami, a to podľa vzoru, ktorý je uvedený v prílohe č. 6.

12.6. Zhotoviteľ sa zaväzuje zaistiť bezpečnosť a odolnosť diela, vrátane akýchkoľvek rozšírení, voči aktuálne známym typom útokov a pred odovzdaním akejkoľvek zmeny diela vykonať testovanie na prítomnosť známych zraniteľností. V prípade zistenia zraniteľností sa zhotoviteľ zaväzuje tieto zraniteľnosti odstrániť, vykonať opätovné testovanie a zdokumentovaný výsledok testovania odovzdať objednávateľovi spolu s vykonaným dielom.

12.7. Zhotoviteľ sa zaväzuje dodržiavať nasledovné bezpečnostné opatrenia a zásady:

i. všetky vstupy aplikácií tvoriacich dielo sú kontrolované na validnosť a sú sanitované;
ii. je zapnutá len nutne potrebná funkcionalita, porty a IP adresy a všetky ostatné sú vypnuté;
iii. v prípade, že je nevyhnutné vykonávať správu diela na diaľku, je to možné vykonávať výhradne prostredníctvom šifrovaných protokolov a každý vzdialený zásah je zdokumentovaný a záznam o zásahu je odovzdaný objednávateľovi najneskôr v posledný deň daného mesiaca;
iv. všetky pôvodné a administrátorské účty sú zdokumentované a majú unikátne prvotné heslo zložené z náhodnej postupnosti aspoň 14 znakov;

v. všetky administrátorské heslá a prístupové údaje a dokumentácia sú k dispozícii aj objednávateľovi (minimálne v zalepenej obálke);
vi. dielo disponuje funkcionalitou pre zmenu používateľských a administrátorských mien a hesiel a funkcionalitou vypnutia používateľského účtu;
vii. všetky komponenty diela sú aktuálne a podporované výrobcom a postup pre aktualizácie a aplikáciu záplat je zdokumentovaný a dodržiavaný;
viii. všetky zmeny v diele sú zdokumentované a dokumentácia a zdrojové kódy sú poskytnuté objednávateľovi bezpečným spôsobom najneskôr v čase nasadenia zmeny do produkčného prostredia;
ix. na vyžiadanie objednávateľa je zhotoviteľ povinný sprístupniť dokumentáciu aktivít zamestnancov zhotoviteľa a tretích strán najneskôr do 24 hodín od požiadavky;
x. na vyžiadanie objednávateľa je zhotoviteľ povinný poskytnúť plnú súčinnosť pri riešení bezpečnostného incidentu povereným zamestnancom objednávateľa či povereným zamestnancom orgánu nadriadenému objednávateľovi;
xi. zhotoviteľ pri výkone činností dbá na vykonávanie svojich činností v súlade s bezpečnostnou dokumentáciou, odporúčaným bezpečnostnými postupmi a v súlade so zásadami due diligence a due care;
xii. zhotoviteľ sa zaväzuje v rámci zachovania kontinuity poskytnúť objednávateľovi prístup k zdrojovým kódom programov vytvorených v rámci plnenia tejto zmluvy.

12.8. Zhotoviteľ je povinný bezodkladne informovať objednávateľa o bezpečnostných udalostiach (identifikovaných stavoch systému, služby alebo siete, ukazujúcich na možné porušenie bezpečnostnej politiky alebo zlyhanie bezpečnostných opatrení vo vzťahu k predmetu tejto zmluvy, pri ktorých však nedošlo k narušeniu dôvernosti, dostupnosti alebo integrity informácií, sietí a služieb) a bezpečnostných incidentoch (udalostiach narúšajúcich dôvernosť, dostupnosť a integritu informácií, fyzickú bezpečnosť priestorov a zariadení objednávateľa, bezpečnosť sietí alebo služieb alebo integritu sietí a služieb vo vzťahu k predmetu tejto zmluvy) a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej a informačnej bezpečnosti na objednávateľa.

12.9. Zhotoviteľ informuje objednávateľa o bezpečnostnej udalosti najneskôr do troch pracovných dní po jej zistení oznámením kontaktnej osobe objednávateľa prostredníctvom elektronickej pošty alebo telefonicky. V prípade bezpečnostného incidentu zhotoviteľ informuje objednávateľa okamžite po jeho zistení, najneskôr do jedného pracovného dňa oznámením kontaktnej osobe objednávateľa telefonicky a zároveň prostredníctvom elektronickej pošty.

12.10. Hlásenie bezpečnostného incidentu obsahuje údaje zhotoviteľa a osoby, ktorá udalosť/incident nahlasuje, názov a popis služby, priestoru, zariadenia alebo informácie, ktorá je predmetom udalosti/incidentu alebo ktorá je narušením ohrozená, prostriedok, poskytujúci službu, zdroj narušenia, ak je známy, cieľ a rozsah narušenia, účastníkov incidentu, ak sú známi, prípadne príslušné prevádzkové záznamy (LOGy) o narušení, ak sú k dispozícii.

12.11. Každý zamestnanec tretej strany resp. tretie osoby realizujúce prácu v súvislosti s naplnením účelu zmluvy (v mene alebo na základe pokynov zhotoviteľa) je povinný pri vyšetrovaní bezpečnostných incidentov zamestnancom alebo zamestnancami objednávateľa, alebo nimi poverenými osobami, poskytnúť potrebnú súčinnosť, za čo zodpovedá zhotoviteľ.

12.12. Po vzniku bezpečnostného incidentu nesmie zamestnanec tretej strany resp. tretia osoba realizujúce prácu v súvislosti s naplnením účelu zmluvy (v mene alebo na základe pokynov zhotoviteľa) vykonávať akékoľvek aktivity, ktoré by mohli viesť k znehodnoteniu dôkazov alebo k zhoršeniu dôsledkov bezpečnostného incidentu, za čo zodpovedá zhotoviteľ.

Článok 13
Skončenie zmluvy

13.1. Zmluvné strany sa dohodli, že túto zmluvu je možné skončiť:

i. písomnou dohodou zmluvných strán, a to dňom uvedeným v takejto dohode, v ktorej sa súčasne upravia nároky zmluvných strán vzniknuté na základe, alebo v súvislosti s touto zmluvou,
ii. písomným odstúpením od zmluvy v prípade podstatného porušenia zmluvy,
iii. písomným odstúpením od zmluvy objednávateľom bez nároku zhotoviteľa na náhradu škody v prípade, kedy ešte nedošlo ani k čiastočnému plneniu zo zmluvy zhotoviteľom a výsledky kontroly riadiaceho orgánu OPII neumožňujú financovanie výdavkov vzniknutých z tejto zmluvy.

13.2. Odstúpenie od zmluvy sa uskutoční písomným oznámením odstupujúcej zmluvnej strany adresovaným druhej zmluvnej strane zároveň s uvedením dôvodu odstúpenia od zmluvy a je účinné okamihom jeho doručenia druhej zmluvnej strane. V prípade pochybností sa má za to, že je odstúpenie doručené tretí deň po jeho odoslaní. Doručuje sa zásadne na adresu zmluvnej strany uvedenú v záhlaví tejto zmluvy.

13.3. Za podstatné porušenie zmluvy sa považuje:

i. omeškanie zhotoviteľa s vykonaním diela oproti dohodnutému termínu plnenia o viac ako šesť (6) týždňov,
ii. ak cena diela bude fakturovaná v rozpore s podmienkami dohodnutými v tejto zmluve,
iii. ak zhotoviteľ vykoná pre objednávateľa dielo takých parametrov, ktoré sú v rozpore s touto zmluvou,
iv. ak objednávateľ je v omeškaní so zaplatením faktúry o viac ako šesťdesiat (60) dní po lehote jej splatnosti,
v. ak zhotoviteľ nevykoná dielo prostredníctvom kľúčových expertov, prostredníctvom ktorých zhotoviteľ ako uchádzač vo verejnom obstarávaní preukazoval splnenie podmienok účasti, resp. prostredníctvom odsúhlasených zmenených kľúčových expertov v súlade so zmluvou.

13.4. Objednávateľ je oprávnený písomne odstúpiť od tejto zmluvy aj v prípade, ak:

i. proti zhotoviteľovi začalo konkurzné konanie alebo reštrukturalizácia,
ii. zhotoviteľ vstúpil do likvidácie,
iii. zhotoviteľ koná v rozpore s touto zmluvou a/alebo všeobecne záväznými právnymi predpismi platnými na území Slovenskej republiky a na písomnú výzvu objednávateľa toto konanie a jeho následky v určenej primeranej lehote neodstráni,
iv. zhotoviteľ nebol v čase uzatvorenia tejto zmluvy alebo počas doby trvania jej platnosti a účinnosti zapísaný v registri partnerov verejného sektora podľa zákona o RPVS,
v. došlo k splneniu zákonných dôvodov na odstúpenie od zmluvy (napr. § 19 ZVO).

13.5. Odstúpenie od zmluvy má následky stanovené príslušnými ustanoveniami Obchodného zákonníka, pokiaľ sa zmluvné strany písomne nedohodnú inak.

Článok 14
Spoločné a záverečné ustanovenia

14.1. Táto zmluva môže byť doplnená alebo zmenená v súlade so všeobecne záväznými právnymi predpismi platnými na území Slovenskej republiky len písomnými a očíslovanými dodatkami, ktoré sa po podpísaní obidvoma zmluvnými stranami stávajú neoddeliteľnou súčasťou tejto zmluvy.

14.2. V ostatných právach a povinnostiach touto zmluvou neupravených platia príslušné ustanovenia Obchodného zákonníka a ostatných všeobecne záväzných právnych predpisov platných na území Slovenskej republiky.

14.3. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z plnenia tejto zmluvy budú riešiť najprv dohodou alebo zmierom. Ak nepríde k dohode, bude vec riešiť vecne a miestne príslušný súd Slovenskej republiky.

14.4. Zmluvné strany vyhlasujú, že túto zmluvu uzatvorili slobodne a vážne, nie v tiesni a za nápadne nevýhodných podmienok, prečítali ju, porozumeli jej a nemajú proti jej forme a obsahu žiadne výhrady, čo potvrdzujú vlastnoručnými podpismi.

14.5. Táto zmluva nadobúda platnosť dňom jej podpisu obidvoma zmluvnými stranami. Táto zmluva nadobudne účinnosť v prípade kumulatívneho splnenia nasledujúcich podmienok:

i. ukončenie finančnej kontroly doručením správy z tejto kontroly objednávateľovi, v rámci ktorej riadiaci orgán OPII neidentifikoval nedostatky, ktoré by mali alebo mohli mať vplyv na výsledok verejného obstarávania, alebo v rámci ktorej objednávateľ súhlasil s výškou ex ante finančnej opravy uvedenej v návrhu správy alebo v správe z kontroly a splnil podmienky na uplatnenie ex ante finančnej opravy podľa metodického pokynu, ktorý upravuje postup pri určení finančných opráv za verejné obstarávanie; za deň splnenia tejto časti odkladacej podmienky sa považuje deň, kedy objednávateľ prostredníctvom systému IS EVO oznámi zhotoviteľovi, že došlo k ukončeniu finančnej kontroly, v rámci ktorej riadiaci orgán neidentifikoval nedostatky, ktoré by mali alebo mohli mať vplyv na výsledok verejného obstarávania (po doručení správy z kontroly objednávateľovi), alebo v rámci ktorej objednávateľ súhlasil s výškou ex ante finančnej opravy uvedenej v návrhu správy alebo v správe z kontroly a splnil podmienky na uplatnenie ex ante finančnej opravy podľa metodického pokynu, ktorý upravuje postup pri určení finančných opráv za verejné obstarávanie a

ii. zverejnenie zmluvy v Centrálnom registri zmlúv.

14.6. Táto zmluva je vyhotovená v štyroch (4) rovnopisoch, z toho dva (2) rovnopisy pre zhotoviteľa a dva (2) rovnopisy pre objednávateľa.

14.7. Neoddeliteľnú súčasť zmluvy tvorí:

i. príloha č. 1 – Opis predmetu zákazky
ii. príloha č. 2 – Vlastný návrh plnenia
iii. príloha č. 3 – Zoznam subdodávateľov
iv. príloha č. 4 – Zoznam kľúčových expertov
v. príloha č. 5 – Záväzný štruktúrovaný rozpočet ceny
vi. príloha č. 6 – Všeobecné podmienky pre zabezpečenie informačnej a kybernetickej bezpečnosti Štatistického úradu Slovenskej republiky

Objednávateľ:	Zhotoviteľ:
Štatistický úrad Slovenskej republiky Ing. Peter Peťko, MBA predseda úradu	SOITRON, s.r.o. Ing. Marián Skákala výkonný riaditeľ a konateľ spoločnosti

Príloha č. 1: Opis predmetu zákazky

1. Predmetom zákazky je:

a) nasadenie bezpečnostných riešení (ďalej aj ako „riešenie“):

- na ochranu auditných záznamov – log manager,
- na ochranu citlivých údajov formou DLP (Data Leakage Prevention),
- na riadenie privilegovaných identít a prístupu k heslám privilegovaných účtov PIM (Privileged Identity Management), a ich overenie v prevádzke,

b) vykonanie posúdenia bezpečnosti prostredia organizácie formou penetračného testovania (ďalej ako „služba“)

(ďalej všetko spolu ako „dielo“).

2. Požiadavky na riešenie a služby

2.1. Log manager

ID	POPIS
LOG 001	Predmetom zákazky má byť riešenie na zabezpečenie správy auditných záznamov (LOG manager) v infraštruktúre IKT v subjekte ŠÚ SR a dodanie a implementácia centrálneho úložiska pre zber a analýzu logov.
LOG 002	Systém musí byť schopný zhromaždiť prevádzkové dáta zo všetkých dôležitých systémov na jednom mieste a dlhodobo ich uchovávať. Týmto operátor IT/Bezpečnosti dostane možnosť zistiť informácie o bezpečnostných incidentoch, prevádzkových stavoch a prípadných chybách v IT v reálnom čase aj v pohľade do minulosti najmenej jeden rok späť.
LOG 003	Riešenie musí byť schopné generovať reporty o aktivitách systémov i užívateľov, vrátane auditných reportov na vyžiadanie, alebo so stanovenou periodicitou s definovateľným obsahom, a to bez nutnosti používať SQL syntax.
LOG 004	Požiadavka je možnosť prechádzania týchto logov integrovaným grafickým rozhraním s preddefinovanými pravidlami pre rýchle vyhľadávanie (napr. ako sú zmeny v systémoch vykonané administrátormi; zoznam novo vytvorených účtov v MS AD za zvolenú periódu; zmeny v prístupových právach pre zadaného užívateľa alebo k zadanej zložke, monitoring privilegovaných účtov, zdieľaných účtov a zmien konfigurácií, sledovanie súborových systémov a pod.)
LOG 005	Systém musí umožňovať sledovať správanie užívateľov a systémov s možnosťou upozorňovania na prekročenie pravidiel, a to na základe limitov alebo korelácií udalostí stanovených administrátorom systému.
LOG 006	Cieľom bude mať jednotné úložisko logov s pokročilými nástrojmi analýzy a upozorňovania, ku ktorému budú mať prístup iba autorizovaní pracovníci organizácie. Nevyhnutnou nutnosťou je vylúčiť možnosť modifikácie logov zo strany administrátorov alebo užívateľov.

LOG 007	Systém musí ďalej umožňovať jednoduchú klasifikáciu dát, tvorbu užívateľsky definovaných parserov, filtrov, upozornení a korelácií bez účasti výrobcu alebo dodávateľa v ľahko pochopiteľnom grafickom rozhraní bez nutnosti používať znalosti programátora.
LOG 008	Dokumentácia k používaniu nástroja musí poskytnúť jednoznačný návod, ako takéto činnosti vykonávať, a to vrátane širokej škály vzorových príkladov.
LOG 009	Zálohovanie konfigurácie aj dát a ich obnova je nevyhnutnou nutnosťou, ktorú musí dodaný systém podporovať.
LOG 010	Pretože nie je dopredu známe presné množstvo logov vznikajúcich v našej organizácii, požadujeme, aby dodaný systém podporoval plánované aj ad-hoc zálohovanie vzniknutých dát na externý zálohovací systém, optimálne za využitia SMB protokolu.
LOG 011	Riešenie pre on-premise inštaláciu vrátene inštalačného manuálu
LOG 012	Programové vybavenie bez licenčnej limitácie počtu logov za jednotku času
LOG 013	Podpora integrácie prostredia MS Windows, Linux
LOG 014	Nástroj musí spĺňať požiadavky Zákona o kybernetickej bezpečnosti a ISO 27001:2013 pre ukladanie auditných záznamov.
LOG 015	Implementácia sa predpokladá min. nad nasledovnými systémami: - IŠIS - IVIS - RPO - MS Exchange - Sieťové prvky ŠÚ SR
LOG 016	Dodanie HW zariadenia s parametrami: - CPU - CPU Mark min. 19000 - RAM min. 128 GB - HDD min. 12*4TB@RAID64 - Záruka minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín
LOG 017	Služby: - dodávka vrátane dopravy na miesto určenia objednávateľom predmetu zákazky - vrátane inštalačných, konfiguračných prác a integrácie do prostredia ŠÚ SR - základné zaškolenie na dodané riešenie - upgrade a update - minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín
LOG 018	Termín najneskôr do 09/2023, najskôr však po vykonaní Penetračného testovania (bod 2.4. tohto opisu predmetu zákazky).

2.2. PIM (Privileged Identity Management)

ID	POPIS
PIM 001	Riešenie má poskytovať nástroj pre správu privilegovaných účtov, riadenie prístupu k týmto účtom a monitoring všetkých aktivít privilegovaných účtov. Užívateľské prístupy budú riadené bezpečnostnou politikou, kedy má vybraný užívateľ práva

	prístupu iba k definovaným účtom a systémom. Účty a systémy, ku ktorým nemá práva prístupu, nie sú pre používateľov viditeľné.
PIM 002	Systém plne podporuje multi-tenant prostredie. Užívatelia/skupiny užívateľov majú prístup iba k vybraným účtom, systémom, auditným záznamom, konfigurácii atp. Aj správca/administrátor riešenia má mať povolený prístup iba k vybraným zložkám a konfigurácii.
PIM 003	Riešenie má umožňovať viacúrovňové schvaľovanie správcovských prístupov k cieľovým systémom - prístupy je možné obmedziť podľa vybraného účtu, alebo na daný časový úsek. Schvaľovanie prístupu je možné vynútiť oddelene pre prístup prihlasovacím údajom privilegovaného účtu, alebo pre pripojenie na koncový systém. O nových žiadostiach, schválení a zamietnutí budú užívatelia upozornení emailom, vytvorením ticketu v helpdesk systéme, atp.
PIM 004	Riešenie musí zaručiť vysokú bezpečnosť prenášaných a uložených informácií (confidentiality, integrity, availability). Uložené informácie, vrátane nahrávok a spravovaným prihlasovacích údajov, budú uložené v jednej centrálnej a zabezpečenej databáze. Riešenie musí umožňovať obmedzenie práv správcu systému tak, aby nemal sám prístup k uloženým prihlasovacím údajom, logom, alebo nahrávkam, bez autorizácie vlastníkov dát.
PIM 005	Správa riešenia bude umožnená pomocou jednotnej centrálnej správy. Riešenie musí umožňovať konfiguráciu systému pomocou RestAPI - správa užívateľov, zakladanie a editácia účtov, zmeny prihlasovacích údajov, terminácia spojenia.
PIM 006	Riešenie ponúka plnú integráciu s Microsoft Active Directory na úrovni informácií o používateľoch, príslušnosti k skupinám a emailoch. Integrácia musí umožňovať mapovanie rolí v PAM riešení v nadväznosti na skupiny v AD.
PIM 007	Prístup k užívateľskému rozhraniu je požadovaný cez webový portál s možnosťou overenia cez LDAP/MS Active Directory. Požaduje sa podpora pre druhý faktor (minimálne PKI karty, RSA ID, Radius server,...).
PIM 008	Riešenie je možné spravovať pomocou Rest API a to minimálne na úrovni - vytváranie užívateľov a účtov, nastavenie oprávnení, zmeny politík, system health monitoring, schvaľovanie požiadaviek, autentizácia.
PIM 009	Nástroj umožňuje dočasné povýšenie oprávnenia bežných (neprivilegovaných) užívateľov na úroveň administrátora na koncových systémoch na platforme MS Windows bez nutnosti inštalácie agentského riešenia. Riešenie umožňuje povýšenie oprávnenia na základe požiadavky, príslušnosti do AD skupiny, prípadne na časovo obmedzené obdobie. Oprávnenia sú následne automaticky odobrané po vopred definovanom intervale.
PIM 010	Riešenie umožňuje vyhľadávať privilegované účty v operačných systémoch/LDAP/MS AD a pridať ich (manuálne aj automaticky) do systému riadenia prístupu podľa bezpečnostnej politiky. Vyhľadávanie účtov nevyužíva inštaláciu agentov na koncové zariadenia.
PIM 011	Riešenie umožňuje automatickú výmenu hesiel a SSH kľúčov privilegovaných účtov po ukončení relácie (jednorazové heslo), alebo v pravidelných intervaloch podľa bezpečnostnej politiky. Rotáciu hesla/SSH kľúča je možné vynútiť aj užívateľom. Heslá a SSH kľúče sa vymieňajú bez použitia agenta/sprostredkovateľa.

PIM 012	Riešenie kontroluje v pravidelných intervaloch zhodu uloženého hesla v systéme riadenia prístupov a cieľovom bode. V prípade nezhody vynúti synchronizáciu, alebo zašle upozornenie správcovi.
PIM 013	Systém umožňuje pravidelné vyhľadávanie účtov, ktoré nie sú riešením spravované, ale sú používané pre prístupy na koncové systémy. Systém takéto účty dokáže vyhľadať, upozorniť na ich použitie a prípadne automaticky zaradiť do správy. Riešenie zároveň umožňuje detekciu nespravovaných účtov v reálnom čase a automatické uloženie a vynútenie zmeny hesla.
PIM 014	Nástroj umožňuje automatickú výmenu hesiel privilegovaných účtov na koncových systémoch s OS MS Windows, ktoré nie sú štandardne pripojené do korporátnej siete. Rotácia hesiel je vynútená lokálne v pravidelných intervaloch podľa bezpečnostnej politiky.
PIM 015	Správcovský prístup na cieľový systém bude sprostredkovaný pomocou tzv. terminal/jump servera prostredníctvom zvoleného komunikačného protokolu, aplikácie a príslušného privilegovaného účtu tak, aby koncový užívateľ nemal prístup k prihlasovacím údajom.
PIM 016	Izolácia prístupu je možná až na úroveň aplikácie (typu webový prehliadač s konkrétnou URL, MMC konzola s vybraným snap-in, konkrétne aplikácie...napr. MS SQL Management Studio, WinSCP..., kedy užívateľ nemá možnosť pristupovať k iným službám , aplikáciám v rámci danej relácie. Po ukončení aplikácie sa uzavrie spojenie celej relácie. Vzdialené pripojenie k relácii je možné nadviazať ako cez vlastné GUI dodaného riešenia, tak aj pomocou štandardných protokolov RDP a SSH a štandardných klientov typu putty a remote desktop manager.
PIM 017	Správcovský prístup prostredníctvom SSH protokolu sa bude vykonávať cez SSH Proxy, kde bude užívateľ overený svojimi prihlasovacími údajmi (je možné spárovať s MS AD) a bude pripojený zvoleným privilegovaným účtom na cieľový systém bez zadávania hesla a podľa bezpečnostnej politiky.
PIM 018	Riešenie poskytuje možnosť pripojenia na vzdialené relácie iba pomocou prehliadača a protokolu HTTPS (nie je teda napríklad nutné otvárať z klientskej stanice RDP/SSH/... protokoly; medzi užívateľom a jump serverom bude vždy otvorený iba bezpečný WebSocket protokol (port 443).
PIM 019	Riešenie musí umožňovať monitoring a nahrávanie celej relácie a aktivít privilegovaných účtov vo video formáte s možnosťou kontextového vyhľadávania, bez nutnosti inštalácie permanentných agentov na koncový systém. Záznam relácie musí byť vytváraný kontinuálne, nie formou screenshotov. V nahrávkach je možné spätne vyhľadávať v zázname vo forme metadát - minimálne pri RDP spustenej aplikácii a udalosti, pri SSH reláciách jednotlivé príkazy, pri Webových aplikáciách click na jednotlivé odkazy, pri iných typoch relácií aspoň stlačenia klávesov. Pre prehrávanie nahrávok nie je potrebná inštalácia nástrojov tretích strán (flash, java, codec, atp...) a je dostupné z GUI dodávaného riešenia.
PIM 020	Systém poskytuje možnosť automaticky vyhodnocovať a označovať nahrávky relácií na základe vybraných spustených príkazov a aplikácií, tak aby bolo možné vyhľadávať potenciálne nebezpečné činnosti. Systém zároveň umožňuje alerting takýchto udalostí, vrátane možnosti exportu logov v reálnom čase pomocou syslog na SIEM.

PIM 021	Riešenie ponúka možnosť automatického pozastavenia, alebo terminácie potenciálne nebezpečných relácií. Pravidlá pre detekciu potenciálne nebezpečných relácií je možné plne editovať – typ udalosti, používatelia (možnosť nastavenia výnimky na úrovni skupín v AD) a typ reakcie.
PIM 022	Riešenie umožňuje sledovať aktívne relácie ďalším užívateľom (napríklad audítor) av prípade potreby ukončiť sledovanú reláciu. Sledovanie "živých" relácií je tiež možné pomocou prehliadača a protokolu HTTPS (nie je nutné otvárať z klientskej stanice RDP protokol).
PIM 023	Systém umožňuje detekciu podozrivých aktivít chovania užívateľov v reálnom čase a musí umožňovať automatické vynútenie nápravných opatrení - alerting, zmena prihlasovacích údajov, terminácia/pozastavenie relácií.
PIM 024	Riešenie umožňuje okamžité zavedenie nových užívateľov do systému. Správca riešení dokáže cez webové rozhranie vytvoriť používateľa, priradiť mu oprávnenie s akými privilegovanými účtami môže disponovať a pre aké časové obdobie. Riešenie následne zašle email novému užívateľovi a umožní mu bezpečné vzdialené pripojenie k PAM riešeniu.
PIM 025	Spojenie medzi externým užívateľom a riešením PIM musí byť plne šifrované. Nie je umožnené priame spojenie medzi stanicou užívateľa a cieľovým systémom - je využitý princíp bezpečného 'jump' servera.
PIM 026	Systém musí umožňovať audit jednotlivých akcií užívateľov s privilegovanými účtami - zobrazenie hesla, zmeny uložených údajov, vytvorenie relácie.
PIM 027	Riešenie musí umožňovať vygenerovanie reportu všetkých aktivít administrátora riešenia.
PIM 028	Riešenie umožňuje nastavenie prístupu k reportom iba pre vybraných užívateľov.
PIM 029	Riešenie musí umožňovať nezmazateľnosť logov po dobu minimálne 30 dní. Auditné záznamy musia byť bezpečne uložené v zašifrovanej podobe, tak aby k nim mal prístup iba oprávnený užívateľ.
PIM 030	Systém musí umožňovať integráciu s nástrojmi log manager a SIEM - prenos logovaných auditných záznamov, najlepšie v reálnom čase pomocou Syslog.
PIM 031	Všetky komponenty riešenia musia spĺňať nároky na vysoké zabezpečenie a automaticky vynucovať tzv. hardening. Úložisko dát, kde sú uložené jednotlivé účty, prihlasovacie údaje, nahrávky relácií a auditné záznamy, je vysoko zabezpečené a oddelené od ostatných komponentov riešenia. Databáza dát je súčasťou riešenia a nie je nutné využívať nástroje tretích strán. Táto požiadavka platí pre všetky údaje v rámci riešenia
PIM 032	Riešenie musí podporovať nasadenie vo vysokej dostupnosti a vlastné technologické možnosti (nie sú používané nástroje/SW tretích strán) pre zabezpečenie High Availability, Disaster Recovery a zálohovanie tak, aby citlivé dáta boli stále vysoko zabezpečené a dostupné iba vlastníkom dát.
PIM 033	Riešenie musí umožňovať bezpečné zálohovanie dát systému - zálohy musia byť šifrované a prístup k zálohovaným dátam je umožnený iba pomocou zabezpečených Disaster Recovery kľúčov.

PIM 034	Riešenie musí byť dimenzované minimálne pre 20 užívateľov s plným užívateľským prístupom (dostupné všetky funkcie riešenia). Licencia nie je obmedzená na počet koncových zariadení alebo riadených účtov. Súčasťou licencie je aj riešenie redundancie všetkých komponentov a taktiež geo-redundancia (aspoň active-passive) s dodatočnou miestnou redundanciou v druhej geolokácii.
PIM 035	Licencia zároveň pokrýva možnosť inštalácie dvoch separátnych testovacích prostredí s plnou funkčnosťou a plným rozsahom.
PIM 036	Služby: - vrátane inštalačných, konfiguračných prác a integrácie do prostredia ŠÚ SR - základné zaškolenie na dodané riešenie - upgrade a update - minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín
PIM 037	- verejný obstarávateľ upozorňuje, že dodá HW, ktorý bude vo vlastníctve ŠÚ SR, s technickými parametrami uvedenými v Prílohe č. 17 týchto súťažných podkladov. - verejný obstarávateľ zároveň upozorňuje, že v prípade, ak sú technické parametre HW nepostačujúce pre uchádzačom navrhnuté riešenie SW, je potrebné rozširujúce komponenty HW uviesť, dodať a naceniť na vlastné náklady v rámci ponuky. Záruka minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín (platí len v prípade rozširujúcich komponentov HW).
PIM 038	Termín dodania najneskôr do 09/2023, najskôr však po vykonaní Penetračného testovania (bod 2.4. tohto opisu predmetu zákazky).

2.3. DLP (Data leakage prevention)

ID	POPIS
DLP 001	Požadujeme dodanie riešenia DLP vo forme programového vybavenia pre koncové zariadenia na platforme MS Windows.
DLP 002	Pred nasadením DLP riešenia na zariadenia musí dodávateľ zmapovať spôsob a formu spracovania dát pomocou modulu tzv. auditor - odkiaľ dáta prichádzajú, ako vznikajú, ako sa s nimi narába a kam putujú ďalej. Počet zariadení je 600.
DLP 003	Riešenie musí reportovať a blokovať aktivity ako: - operácie so súbormi - práca s elektronickou poštou a prístupom do siete Internet - využívanie aplikácií - využívanie tlačiarní (virtuálne lokálne sieťové) - práca s pevnými diskami a pamäťovými médiami všeobecne - prenos súborov po sieti
DLP 004	Požadovaná je integrácia s MS AD
DLP 005	Požadovaná je ochrana proti zastaveniu samotného programového vybavenia, ochrana proti odinštalovaniu služby, ochrana proti editácii registrov, systémových komponentov a knižníc. Ochrana proti zmene nastavenia a techniky na reštart a obnovu služby.

DLP 006	Riešenie musí zabezpečiť funkčnosť podľa prednastavených politík aj v offline móde.
DLP 007	Riešenie musí generovať výstrahy formou elektronickej pošty v prípade identifikovaných bezpečnostných incidentov.
DLP 008	Riešenie musí poskytnúť detailné informácie o využívaných aplikáciách, a poskytnúť kategorizáciu aplikácií.
DLP 009	Riešenie musí na základe definície kategórie citlivých dát obmedziť pohyb a prácu s týmito dátami.
DLP 010	Riešenie musí umožniť konfiguráciu politík pre vybrané aplikácie vo forme definície zdroja a cieľa užívateľských operácií.
DLP 011	Možnosť úplne blokovať užívateľské operácie, informovať užívateľa notifikáciami, logovať užívateľské akcie.
DLP 012	Možnosť definovať citlivé dáta pomocou preddefinovaných slovníkov a algoritmov, vlastných reťazcov a regulárnych výrazov.
DLP 013	Možnosť importu vlastných slovníkov.
DLP 014	Dynamické reštrikcie nad súbormi a aplikáciami na základe detekovaného citlivého obsahu.
DLP 015	Blokovanie odosielania citlivých dát mimo koncovú stanicu, komunikačnými cestami ako email, web, externé zariadenie, IM.
DLP 016	Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov.
DLP 017	Podpora : - MS Windows 7, 8.1, 10 a 11 - serverových operačných systémov Windows server 2016, 2019 a 2022 - terminálových prostredí
DLP 018	Centrálna administrátorská konzola, multitenantná administrácia v súlade s organizačným členením subjektov na úrovni domény
DLP 019	Riadené užívateľské práva do nastavení konzoly, k výsledným logom a administrácie riešenia
DLP 020	Skrytý režim na koncovej stanici vrátane procesov a zložiek, a to vrátane lokálnych a doménových administrátorov
DLP 021	Služby: - vrátane inštalačných, konfiguračných prác a integrácie do prostredia ŠÚ SR - základné zaškolenie na dodané riešenie - upgrade a update - minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín
DLP 022	- verejný obstarávateľ upozorňuje, že dodá HW, ktorý bude vo vlastníctve ŠÚ SR, s technickými parametrami uvedenými v Prílohe č. 17 týchto súťažných podkladov. - verejný obstarávateľ zároveň upozorňuje, že v prípade, ak sú technické parametre HW nepostačujúce pre uchádzačom navrhnuté riešenie SW, je potrebné rozširujúce komponenty HW uviesť, dodať a naceniť na vlastné

	náklady v rámci ponuky. Záruka minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín (platí len v prípade rozširujúcich komponentov HW).
DLP 023	Termín najneskôr do 09/2023, najskôr však po vykonaní Penetračného testovania (bod 2.4. tohto opisu predmetu zákazky).

2.4. Penetračné testovanie

ID	POPIS
PEN 001	Aplikačná bezpečnosť - weboveho serveru Cieľ testu je čo najdôkladnejšie a najdetailnejšie otestovať webové aplikácie a webové servre (všetky formuláre, všetky druhy známych zraniteľností).
PEN 001.1	- praktická "hackerská" demonštrácia odhalených kritických zraniteľností (tvorba vlastných "exploit" programov, dump databázy, demonštrácia CSRF/XSS/Session fixation zraniteľností atď)
PEN 001.2	- kompletné a úplné otestovanie webových aplikácií podľa testovacej príručky OWASP 30
PEN 002	Sieťová bezpečnosť - externý test Test je realizovaný z pohľadu potenciálneho anonymného útočníka z Internetu, ktorý nedisponuje žiadnymi informáciami o testovanej topológii a testovaných službách.
PEN 002.1	- Kontrola zraniteľností – vykonanie bezpečnostného scanu na odhalenie dostupných existujúcich zraniteľností v službách zistených počas porstcanu
PEN 002.2	- Prienik – snaha o zneužitie dostupných zraniteľností a nedostatočnej konfigurácie za účelom prieniku do ostatných systémov a zariadení, zvýšenia užívateľských oprávnení a prístupu k prostriedkom
PEN 002.3	- Zbieranie Informácií – o cieľovom systéme sú zozbierané, identifikované a analyzované všetky informácie, vrátane verzie webového serveru, použitých modulov, programovej platformy, WAF a prístupových bodov do aplikácie
PEN 002.4	- Enumerovanie a mapovanie zraniteľností – pomocou intruzívnych metód a techník (špeciálne skonštruované HTTP žiadosti) sú identifikované potenciálne slabiny (použité sú špeciálne bezpečnostné scannery, "fault-injection proxies" ako aj manuálne overenie)
PEN 002.5	- Využitie zraniteľností – pokus o získanie prístupu pomocou zraniteľností identifikovaných v predchádzajúcej fáze. Cieľom je získať používateľský alebo privilegovaný (administrátorsky) prístup do aplikácie alebo operačného systému (použité sú špeciálne "exploit" skripty a "exploit" systémy
PEN 002.6	- Testovanie poštového serveru – okrem testovania známych zraniteľností v konkrétnej implementácii MTA servera, je realizovaných niekoľko detailných SMTP testov na overenie „relaying problémov" MTA servera, takže sú odhalené všetky možnosti zneužitia SMTP servera prípadným spamerom a odolnosti MTA servera na potenciálny DOS útok. Test sa vzťahuje na všetky MX servery pre danú testovanú doménu. Súčasne sú otestované potenciálne zneužiteľné zraniteľnosti antivírových a antispamových implementácií.
PEN 002.7	- Testovanie DNS zón – okrem testovania známych zraniteľností v konkrétnej implementácii DNS servera (Bind, Microsoft DNS server) je realizovaný tiež test konzistencie zón na všetkých zadaných DNS serveroch, kontrola možnosti verejného „zone transfer", zraniteľnosť na DNS „caching" útoky atď. Súčasne sú realizované detailné penetračné testy každého DNS servera pre danú doménu (aj mimo siete objednávateľa – v tomto prípade je nutný ale súhlas príslušného prevádzkovateľa).

PEN 003	Sieťová bezpečnosť - interný test Test je realizovaný z pohľadu potenciálneho anonymného útočníka z vnútra organizácie, ktorý nedisponuje žiadnymi informáciami o testovanej topológii a testovaných službách.
PEN 003.1	- Kontrola zraniteľností – vykonanie bezpečnostného skenu na odhalenie dostupných existujúcich zraniteľností v službách zistených počas portscanu
PEN 003.2	- Prienik – snaha o zneužitie dostupných zraniteľností a nedostatočnej konfigurácie za účelom prieniku do ostatných systémov a zariadení, zvýšenia užívateľských oprávnení a prístupu k prostriedkom
PEN 003.3	- Zbieranie Informácií – o cieľovom systéme sú zozbierané, identifikované a analyzované všetky informácie, vrátane verzie webového serveru, použitých modulov, programovej platformy, WAF a prístupových bodov do aplikácie
PEN 003.4	- Enumerácia a mapovanie zraniteľností – pomocou intruzívnych metód a techník (špeciálne skonštruované HTTP žiadosti) sú identifikované potenciálne slabiny (použité sú špeciálne bezpečnostné scannery, “fault-injection proxies” ako aj manuálne overenie)
PEN 003.5	- Využitie zraniteľností – pokus o získanie prístupu pomocou zraniteľností identifikovaných v predchádzajúcej fáze. Cieľom je získať používateľský alebo privilegovaný (administrátorsky) prístup do aplikácie alebo operačného systému (použité sú špeciálne “exploit” skripty a “exploit” systémy technická výsledná správa s manažérskym zhrnutím, so všetkými odhalenými zraniteľnostami, ich stupňami rizík a odporučeniami
PEN 004	Vulnerability sken datacentra - cloud services
PEN 004.1	- vulnerability internal sken datacentra(jedna lokalita) - cloud services
PEN 004.2	- inštalácia sondy, zber údajov, vyhodnotenie, report.
PEN 005	Sociálne inžinierstvo
PEN 005.1	- fyzický prienik do budovy (príprava + realizácia)
PEN 005.2	- plošná phishingová kampaň
PEN 005.3	- spearphishing (10 zamestnancov ŠÚ SR)
PEN 005.4	- telefonický socialing
PEN 005.5	- USB/keyloggers (príprava + rozmiestenie na 3 lokality)
PEN 006	Penetračné testovanie je akceptované ako celok – t. j. musia byť vykonané všetky druhy uvedených penetračných testov.
PEN 007	Penetračné testovanie je nutné realizovať pred nasadením riešení (log manager, PIM, DLP) – najneskôr však do 3 mesiacov od účinnosti zmluvy.

2.5. Spoločné ustanovenia

Na dodaní diela sa budú priamo podieľať títo kľúčoví experti:
Kľúčový expert č. 1 – Projektový manažér
Kľúčový expert č. 2 – Bezpečnostný architekt riešenia
Kľúčový expert č. 3 – Expert na implementáciu log manažmentu a SIEM (Security Information and Event Management)
Kľúčový expert č. 4 – Expert na implementáciu PIM (Privileged Identitiy Management)

Kľúčový expert č. 5 – Expert na implementáciu DLP (Data Leakage Prevention)

3. Sledované ciele

Na rozdiel od súčasného stavu ŠÚ SR bude disponovať v cieľovom stave rádovo vyššou schopnosťou detekcie škodlivých aktivít, technologické vybavenie a služby ŠÚ SR budú umožňovať lepšiu ochranu pred útokmi z externého prostredia a ochranu spracovávaných dát.

4. Legislatívny rámec

- zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- § 15 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení – bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. k) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 287/2021 Z. z.,
- zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- príloha č. 2 vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy (Minimálne bezpečnostné opatrenia).

Príloha č. 2: Vlastný návrh plnenia

Požiadavky na riešenie a služby

Log manager

ID	Popis	Splnenie požiadaviek (áno/nie) *vyplní uchádzač*	Vlastný návrh riešenia/plnenia predmetu zákazky *vyplní uchádzač*
LOG 001	Predmetom zákazky má byť riešenie na zabezpečenie správy auditných záznamov (LOG manager) v infraštruktúre IKT v subjekte ŠÚ SR a dodanie a implementácia centrálneho úložiska pre zber a analýzu logov.	ÁNO	Logmanager L
LOG 002	Systém musí byť schopný zhromaždiť prevádzkové dáta zo všetkých dôležitých systémov na jednom mieste a dlhodobo ich uchovávať. Týmto operátor IT/Bezpečnosti dostane možnosť zistiť informácie o bezpečnostných incidentoch, prevádzkových stavoch a prípadných chybách v IT v reálnom čase aj v pohľade do minulosti najmenej jeden rok späť.	ÁNO	Systém zhromazdi prevádzkové dáta zo všetkých dôležitých systémov na jednom mieste a dlhodobo ich uchovávať. Týmto operátor IT/Bezpečnosti dostane možnosť zistiť informácie o bezpečnostných incidentoch, prevádzkových stavoch a prípadných chybách v IT v reálnom čase aj v pohľade do minulosti najmenej jeden rok späť.
LOG 003	Riešenie musí byť schopné generovať reporty o aktivitách systémov i užívateľov, vrátane auditných reportov na vyžiadanie, alebo so stanovenou periodicitou s definovateľným obsahom, a to bez nutnosti používať SQL syntax.	ÁNO	Riešenie generuje reporty o aktivitách systémov i užívateľov, vrátane auditných reportov na vyžiadanie, alebo so stanovenou periodicitou s definovateľným obsahom, a to bez nutnosti používať SQL syntax.
LOG 004	Požiadavka je možnosť prechádzania týchto logov integrovaným grafickým rozhraním s preddefinovanými pravidlami pre rýchle vyhľadávanie (napr. ako sú zmeny v systémoch vykonané administrátormi; zoznam novo vytvorených účtov v MS AD za zvolenú periódu; zmeny v prístupových právach pre zadaného užívateľa alebo k zadanej zložke, monitoring privilegovaných účtov, zdieľaných účtov a zmien konfigurácií, sledovanie súborových systémov a pod.)	ÁNO	Riesenie umoznuje prechádzania týchto logov integrovaným grafickým rozhraním s preddefinovanými pravidlami pre rýchle vyhľadávanie (napr. ako sú zmeny v systémoch vykonané administrátormi; zoznam novo vytvorených účtov v MS AD za zvolenú periódu; zmeny v prístupových právach pre zadaného užívateľa alebo k zadanej zložke, monitoring privilegovaných účtov, zdieľaných účtov a zmien konfigurácií, sledovanie súborových systémov a pod.)
LOG 005	Systém musí umožňovať sledovať správanie užívateľov a systémov s možnosťou upozorňovania na prekročenie pravidiel, a to na základe limitov alebo korelácií udalostí stanovených administrátorom systému.	ÁNO	Systém umoznuje sledovať správanie užívateľov a systémov s možnosťou upozorňovania na prekročenie pravidiel, a to na základe limitov alebo korelácií udalostí stanovených administrátorom systému.
LOG 006	Cieľom bude mať jednotné úložisko logov s pokročilými nástrojmi analýzy a upozorňovania, ku ktorému budú mať prístup iba autorizovaní pracovníci organizácie. Nevyhnutnou nutnosťou je vylúčiť možnosť modifikácie logov zo strany administrátorov alebo užívateľov.	ÁNO	jednotné úložisko logov s pokročilými nástrojmi analýzy a upozorňovania, ku ktorému budú mať prístup iba autorizovaní pracovníci organizácie. Nevyhnutnou nutnosťou je vylúčiť možnosť modifikácie logov zo strany administrátorov alebo užívateľov.
LOG 007	Systém musí ďalej umožňovať jednoduchú klasifikáciu dát, tvorbu užívateľsky definovaných parserov, filtrov, upozornení a korelácií bez účasti výrobcu alebo dodávateľa v ľahko pochopiteľnom grafickom rozhraní bez nutnosti používať znalosti programátora.	ÁNO	Systém umoznuje jednoduchú klasifikáciu dát, tvorbu užívateľsky definovaných parserov, filtrov, upozornení a korelácií bez účasti výrobcu alebo dodávateľa v ľahko pochopiteľnom grafickom rozhraní bez nutnosti používať znalosti programátora.
LOG 008	Dokumentácia k používaniu nástroja musí poskytnúť jednoznačný návod, ako takéto činnosti vykonávať, a to vrátane širokej škály vzorových príkladov.	ÁNO	Dokumentácia poskytuje jednoznačný návod, ako takéto činnosti vykonávať, a to vrátane širokej škály vzorových príkladov.
LOG 009	Zálohovanie konfigurácie aj dát a ich obnova je nevyhnutnou nutnosťou, ktorú musí dodaný systém podporovať.	ÁNO	System umoznuje zálohovanie konfigurácie aj dát a ich obnovu.

LOG 010	Pretože nie je dopredu známe presné množstvo logov vznikajúcich v našej organizácii, požadujeme, aby dodaný systém podporoval plánované aj ad-hoc zálohovanie vzniknutých dát na externý zálohovací systém, optimálne za využitia SMB protokolu.	ÁNO	riesenie umoznuje pozadovanu zalohu.
LOG 011	Riešenie pre on-premise inštaláciu vrátene inštalačného manuálu	ÁNO	on premise instalacia
LOG 012	Programové vybavenie bez licenčnej limitácie počtu logov za jednotku času	ÁNO	riesenie bez licencnej limitacie eps
LOG 013	Podpora integrácie prostredia MS Windows, Linux	ÁNO	Podpora integrácie prostredia MS Windows, Linux
LOG 014	Nástroj musí spĺňať požiadavky Zákona o kybernetickej bezpečnosti a ISO 27001:2013 pre ukladanie auditných záznamov.	ÁNO	Nástroj splna požiadavky Zákona o kybernetickej bezpečnosti a ISO 27001:2013 pre ukladanie auditných záznamov.
LOG 015	Implementácia sa predpokladá min. nad nasledovnými systémami: - IŠIS - IVIS - RPO - MS Exchange - Sieťové prvky ŠÚ SR	ÁNO	ano
LOG 016	Dodanie HW zariadenia s parametrami: - CPU - CPU Mark min. 19000 - RAM min. 128 GB - HDD min. 12*4TB@RAID64 - Záruka minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín	ÁNO	HW zariadenie s parametrami: - CPU - CPU Mark min. 19000 - RAM min. 128 GB - HDD min. 12*4TB@RAID64 - Záruka minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín
LOG 017	Služby: - dodávka vrátane dopravy na miesto určenia objednávateľom predmetu zákazky - vrátane inštalačných, konfiguračných prác a integrácie do prostredia ŠÚ SR - základné zaškolenie na dodané riešenie - upgrade a update - minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín	ÁNO	Služby: - dodávka vrátane dopravy na miesto určenia objednávateľom predmetu zákazky - vrátane inštalačných, konfiguračných prác a integrácie do prostredia ŠÚ SR - základné zaškolenie na dodané riešenie - upgrade a update - minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín
LOG 018	Termín najneskôr do 09/2023, najskôr však po vykonaní Penetračného testovania (bod 2.4. opisu predmetu zákazky).	ÁNO	Uchádzač nevyplňa Vlastný návrh riešenia/plnenia predmetu zákazky pri LOG 018

PIM (Privileged Identity Management)

ID	**Popis**	**Splnenie požiadaviek (áno/nie)** *vyplní uchádzač*	**Vlastný návrh riešenia/plnenia predmetu zákazky** *vyplní uchádzač*
PIM 001	Riešenie má poskytovať nástroj pre správu privilegovaných účtov, riadenie prístupu k týmto účtom a monitoring všetkých aktivít privilegovaných účtov. Užívateľské prístupy budú riadené bezpečnostnou politikou, kedy má vybraný užívateľ práva prístupu iba k definovaným účtom a systémom. Účty a systémy, ku ktorým nemá práva prístupu, nie sú pre používateľov viditeľné.	ÁNO	CyberArk PAS

PIM 002	Systém plne podporuje multi-tenant prostredie. Užívatelia/skupiny užívateľov majú prístup iba k vybraným účtom, systémom, auditným záznamom, konfigurácii atp. Aj správca/administrátor riešenia má mať povolený prístup iba k vybraným zložkám a konfigurácii.	ÁNO	Systém plne podporuje multi-tenant prostredie. Užívatelia/skupiny užívateľov majú prístup iba k vybraným účtom, systémom, auditným záznamom, konfigurácii atp. Aj správca/administrátor riešenia má mať povolený prístup iba k vybraným zložkám a konfigurácii.
PIM 003	Riešenie má umožňovať viacúrovňové schvaľovanie správcovských prístupov k cieľovým systémom - prístupy je možné obmedziť podľa vybraného účtu, alebo na daný časový úsek. Schvaľovanie prístupu je možné vynútiť oddelene pre prístup prihlasovacím údajom privilegovaného účtu, alebo pre pripojenie na koncový systém. O nových žiadostiach, schválení a zamietnutí budú užívatelia upozornení emailom, vytvorením ticketu v helpdesk systéme, atp.	ÁNO	Riešenie umoznuje viacúrovňové schvaľovanie správcovských prístupov k cieľovým systémom - prístupy je možné obmedziť podľa vybraného účtu, alebo na daný časový úsek. Schvaľovanie prístupu je možné vynútiť oddelene pre prístup prihlasovacím údajom privilegovaného účtu, alebo pre pripojenie na koncový systém. O nových žiadostiach, schválení a zamietnutí budú užívatelia upozornení emailom, vytvorením ticketu v helpdesk systéme, atp.
PIM 004	Riešenie musí zaručiť vysokú bezpečnosť prenášaných a uložených informácií (confidentiality, integrity, availability). Uložené informácie, vrátane nahrávok a spravovaným prihlasovacích údajov, budú uložené v jednej centrálnej a zabezpečenej databáze. Riešenie musí umožňovať obmedzenie práv správcu systému tak, aby nemal sám prístup k uloženým prihlasovacím údajom, logom, alebo nahrávkam, bez autorizácie vlastníkov dát.	ÁNO	Riešenie podporuje vysokú bezpečnosť prenášaných a uložených informácií (confidentiality, integrity, availability). Uložené informácie, vrátane nahrávok a spravovaným prihlasovacích údajov, budú uložené v jednej centrálnej a zabezpečenej databáze. Riešenie musí umožňovať obmedzenie práv správcu systému tak, aby nemal sám prístup k uloženým prihlasovacím údajom, logom, alebo nahrávkam, bez autorizácie vlastníkov dát.
PIM 005	Správa riešenia bude umožnená pomocou jednotnej centrálnej správy. Riešenie musí umožňovať konfiguráciu systému pomocou RestAPI - správa užívateľov, zakladanie a editácia účtov, zmeny prihlasovacích údajov, terminácia spojenia.	ÁNO	Riesenie ma centralnu spravu s pozadovanymi vlastnostami
PIM 006	Riešenie ponúka plnú integráciu s Microsoft Active Directory na úrovni informácií o používateľoch, príslušnosti k skupinám a emailoch. Integrácia musí umožňovať mapovanie rolí v PAM riešení v nadväznosti na skupiny v AD.	ÁNO	Riešenie ponúka plnú integráciu s Microsoft Active Directory na úrovni informácií o používateľoch, príslušnosti k skupinám a emailoch. Riesenie umoznuje mapovanie rolí v PAM riešení v nadväznosti na skupiny v AD.
PIM 007	Prístup k užívateľskému rozhraniu je požadovaný cez webový portál s možnosťou overenia cez LDAP/MS Active Directory. Požaduje sa podpora pre druhý faktor (minimálne PKI karty, RSA ID, Radius server,...).	ÁNO	Prístup k užívateľskému rozhraniu je cez webový portál s možnosťou overenia cez LDAP/MS Active Directory. Riesenie ma podporu pre druhý faktor (MFA).
PIM 008	Riešenie je možné spravovať pomocou Rest API a to minimálne na úrovni - vytváranie užívateľov a účtov, nastavenie oprávnení, zmeny politík, system health monitoring, schvaľovanie požiadaviek, autentizácia.	ÁNO	Riešenie je možné spravovať pomocou Rest API a to minimálne na úrovni - vytváranie užívateľov a účtov, nastavenie oprávnení, zmeny politík, system health monitoring, schvaľovanie požiadaviek, autentizácia.
PIM 009	Nástroj umožňuje dočasné povýšenie oprávnenia bežných (neprivilegovaných) užívateľov na úroveň administrátora na koncových systémoch na platforme MS Windows bez nutnosti inštalácie agentského riešenia. Riešenie umožňuje povýšenie oprávnenia na základe požiadavky, príslušnosti do AD skupiny, prípadne na časovo obmedzené obdobie. Oprávnenia sú následne automaticky odobrané po vopred definovanom intervale.	ÁNO	Nástroj umožňuje dočasné povýšenie oprávnenia bežných (neprivilegovaných) užívateľov na úroveň administrátora na koncových systémoch na platforme MS Windows bez nutnosti inštalácie agentského riešenia. Riešenie umožňuje povýšenie oprávnenia na základe požiadavky, príslušnosti do AD skupiny, prípadne na časovo obmedzené obdobie. Oprávnenia sú následne automaticky odobrané po vopred definovanom intervale.
PIM 010	Riešenie umožňuje vyhľadávať privilegované účty v operačných systémoch/LDAP/MS AD a pridať ich (manuálne aj automaticky) do systému riadenia prístupu podľa bezpečnostnej politiky. Vyhľadávanie účtov nevyužíva inštaláciu agentov na koncové zariadenia.	ÁNO	Riešenie umožňuje vyhľadávať privilegované účty v operačných systémoch/LDAP/MS AD a pridať ich (manuálne aj automaticky) do systému riadenia prístupu podľa bezpečnostnej politiky. Vyhľadávanie účtov nevyužíva inštaláciu agentov na koncové zariadenia.

PIM 011	Riešenie umožňuje automatickú výmenu hesiel a SSH kľúčov privilegovaných účtov po ukončení relácie (jednorazové heslo), alebo v pravidelných intervaloch podľa bezpečnostnej politiky. Rotáciu hesla/SSH kľúča je možné vynútiť aj užívateľom. Heslá a SSH kľúče sa vymieňajú bez použitia agenta/sprostredkovateľa.	ÁNO	Riešenie umožňuje automatickú výmenu hesiel a SSH kľúčov privilegovaných účtov po ukončení relácie (jednorazové heslo), alebo v pravidelných intervaloch podľa bezpečnostnej politiky. Rotáciu hesla/SSH kľúča je možné vynútiť aj užívateľom. Heslá a SSH kľúče sa vymieňajú bez použitia agenta/sprostredkovateľa.
PIM 012	Riešenie kontroluje v pravidelných intervaloch zhodu uloženého hesla v systéme riadenia prístupov a cieľovom bode. V prípade nezhody vynúti synchronizáciu, alebo zašle upozornenie správcovi.	ÁNO	Riešenie kontroluje v pravidelných intervaloch zhodu uloženého hesla v systéme riadenia prístupov a cieľovom bode. V prípade nezhody vynúti synchronizáciu, alebo zašle upozornenie správcovi.
PIM 013	Systém umožňuje pravidelné vyhľadávanie účtov, ktoré nie sú riešením spravované, ale sú používané pre prístupy na koncové systémy. Systém takéto účty dokáže vyhľadať, upozorniť na ich použitie a prípadne automaticky zaradiť do správy. Riešenie zároveň umožňuje detekciu nespravovaných účtov v reálnom čase a automatické uloženie a vynútenie zmeny hesla.	ÁNO	Systém umožňuje pravidelné vyhľadávanie účtov, ktoré nie sú riešením spravované, ale sú používané pre prístupy na koncové systémy. Systém takéto účty dokáže vyhľadať, upozorniť na ich použitie a prípadne automaticky zaradiť do správy. Riešenie zároveň umožňuje detekciu nespravovaných účtov v reálnom čase a automatické uloženie a vynútenie zmeny hesla.
PIM 014	Nástroj umožňuje automatickú výmenu hesiel privilegovaných účtov na koncových systémoch s OS MS Windows, ktoré nie sú štandardne pripojené do korporátnej siete. Rotácia hesiel je vynútená lokálne v pravidelných intervaloch podľa bezpečnostnej politiky.	ÁNO	Nástroj umožňuje automatickú výmenu hesiel privilegovaných účtov na koncových systémoch s OS MS Windows, ktoré nie sú štandardne pripojené do korporátnej siete. Rotácia hesiel je vynútená lokálne v pravidelných intervaloch podľa bezpečnostnej politiky.
PIM 015	Správcovský prístup na cieľový systém bude sprostredkovaný pomocou tzv. terminal/jump servera prostredníctvom zvoleného komunikačného protokolu, aplikácie a príslušného privilegovaného účtu tak, aby koncový užívateľ nemal prístup k prihlasovacím údajom.	ÁNO	Správcovský prístup na cieľový systém bude sprostredkovaný pomocou tzv. terminal/jump servera prostredníctvom zvoleného komunikačného protokolu, aplikácie a príslušného privilegovaného účtu tak, aby koncový užívateľ nemal prístup k prihlasovacím údajom.
PIM 016	Izolácia prístupu je možná až na úroveň aplikácie (typu webový prehliadač s konkrétnou URL, MMC konzola s vybraným snap-in, konkrétne aplikácie...napr. MS SQL Management Studio, WinSCP..., kedy užívateľ nemá možnosť pristupovať k iným službám , aplikáciám v rámci danej relácie. Po ukončení aplikácie sa uzavrie spojenie celej relácie. Vzdialené pripojenie k relácii je možné nadviazať ako cez vlastné GUI dodaného riešenia, tak aj pomocou štandardných protokolov RDP a SSH a štandardných klientov typu putty a remote desktop manager.	ÁNO	Izolácia prístupu je možná až na úroveň aplikácie (typu webový prehliadač s konkrétnou URL, MMC konzola s vybraným snap-in, konkrétne aplikácie...napr. MS SQL Management Studio, WinSCP..., kedy užívateľ nemá možnosť pristupovať k iným službám , aplikáciám v rámci danej relácie. Po ukončení aplikácie sa uzavrie spojenie celej relácie. Vzdialené pripojenie k relácii je možné nadviazať ako cez vlastné GUI dodaného riešenia, tak aj pomocou štandardných protokolov RDP a SSH a štandardných klientov typu putty a remote desktop manager.
PIM 017	Správcovský prístup prostredníctvom SSH protokolu sa bude vykonávať cez SSH Proxy, kde bude užívateľ overený svojimi prihlasovacími údajmi (je možné spárovať s MS AD) a bude pripojený zvoleným privilegovaným účtom na cieľový systém bez zadávania hesla a podľa bezpečnostnej politiky.	ÁNO	Správcovský prístup prostredníctvom SSH protokolu sa bude vykonávať cez SSH Proxy, kde bude užívateľ overený svojimi prihlasovacími údajmi (je možné spárovať s MS AD) a bude pripojený zvoleným privilegovaným účtom na cieľový systém bez zadávania hesla a podľa bezpečnostnej politiky.
PIM 018	Riešenie poskytuje možnosť pripojenia na vzdialené relácie iba pomocou prehliadača a protokolu HTTPS (nie je teda napríklad nutné otvárať z klientskej stanice RDP/SSH/... protokoly; medzi užívateľom a jump serverom bude vždy otvorený iba bezpečný WebSocket protokol (port 443).	ÁNO	Riešenie poskytuje možnosť pripojenia na vzdialené relácie iba pomocou prehliadača a protokolu HTTPS (nie je teda napríklad nutné otvárať z klientskej stanice RDP/SSH/... protokoly; medzi užívateľom a jump serverom bude vždy otvorený iba bezpečný WebSocket protokol (port 443).

PIM 019	Riešenie musí umožňovať monitoring a nahrávanie celej relácie a aktivít privilegovaných účtov vo video formáte s možnosťou kontextového vyhľadávania, bez nutnosti inštalácie permanentných agentov na koncový systém. Záznam relácie musí byť vytváraný kontinuálne, nie formou screenshotov. V nahrávkach je možné spätne vyhľadávať v zázname vo forme metadát - minimálne pri RDP spustenej aplikácii a udalosti, pri SSH reláciách jednotlivé príkazy, pri Webových aplikáciách click na jednotlivé odkazy, pri iných typoch relácií aspoň stlačenia klávesov. Pre prehrávanie nahrávok nie je potrebná inštalácia nástrojov tretích strán (flash, java, codec, atp...) a je dostupné z GUI dodávaného riešenia.	ÁNO	Riešenie umoznuje monitoring a nahrávanie celej relácie a aktivít privilegovaných účtov vo video formáte s možnosťou kontextového vyhľadávania, bez nutnosti inštalácie permanentných agentov na koncový systém. Záznam relácie je vytváraný kontinuálne. V nahrávkach je možné spätne vyhľadávať v zázname vo forme metadát - minimálne pri RDP spustenej aplikácii a udalosti, pri SSH reláciách jednotlivé príkazy, pri Webových aplikáciách click na jednotlivé odkazy, pri iných typoch relácií aspoň stlačenia klávesov. Pre prehrávanie nahrávok nie je potrebná inštalácia nástrojov tretích strán (flash, java, codec, atp...) a je dostupné z GUI dodávaného riešenia.
PIM 020	Systém poskytuje možnosť automaticky vyhodnocovať a označovať nahrávky relácií na základe vybraných spustených príkazov a aplikácií, tak aby bolo možné vyhľadávať potenciálne nebezpečné činnosti. Systém zároveň umožňuje alerting takýchto udalostí, vrátane možnosti exportu logov v reálnom čase pomocou syslog na SIEM.	ÁNO	Systém poskytuje možnosť automaticky vyhodnocovať a označovať nahrávky relácií na základe vybraných spustených príkazov a aplikácií, tak aby bolo možné vyhľadávať potenciálne nebezpečné činnosti. Systém zároveň umožňuje alerting takýchto udalostí, vrátane možnosti exportu logov v reálnom čase pomocou syslog na SIEM.
PIM 021	Riešenie ponúka možnosť automatického pozastavenia, alebo terminácie potenciálne nebezpečných relácií. Pravidlá pre detekciu potenciálne nebezpečných relácií je možné plne editovať – typ udalosti, používatelia (možnosť nastavenia výnimky na úrovni skupín v AD) a typ reakcie.	ÁNO	Riešenie ponúka možnosť automatického pozastavenia, alebo terminácie potenciálne nebezpečných relácií. Pravidlá pre detekciu potenciálne nebezpečných relácií je možné plne editovať – typ udalosti, používatelia (možnosť nastavenia výnimky na úrovni skupín v AD) a typ reakcie.
PIM 022	Riešenie umožňuje sledovať aktívne relácie ďalším užívateľom (napríklad audítor) av prípade potreby ukončiť sledovanú reláciu. Sledovanie "živých" relácií je tiež možné pomocou prehliadača a protokolu HTTPS (nie je nutné otvárať z klientskej stanice RDP protokol).	ÁNO	Riešenie umožňuje sledovať aktívne relácie ďalším užívateľom (napríklad audítor) av prípade potreby ukončiť sledovanú reláciu. Sledovanie "živých" relácií je tiež možné pomocou prehliadača a protokolu HTTPS (nie je nutné otvárať z klientskej stanice RDP protokol).
PIM 023	Systém umožňuje detekciu podozrivých aktivít chovania užívateľov v reálnom čase a musí umožňovať automatické vynútenie nápravných opatrení - alerting, zmena prihlasovacích údajov, terminácia/pozastavenie relácií.	ÁNO	Systém umožňuje detekciu podozrivých aktivít chovania užívateľov v reálnom čase a musí umožňovať automatické vynútenie nápravných opatrení - alerting, zmena prihlasovacích údajov, terminácia/pozastavenie relácií.
PIM 024	Riešenie umožňuje okamžité zavedenie nových užívateľov do systému. Správca riešení dokáže cez webové rozhranie vytvoriť používateľa, priradiť mu oprávnenie s akými privilegovanými účtami môže disponovať a pre aké časové obdobie. Riešenie následne zašle email novému užívateľovi a umožní mu bezpečné vzdialené pripojenie k PAM riešeniu.	ÁNO	Riešenie umožňuje okamžité zavedenie nových užívateľov do systému. Správca riešení dokáže cez webové rozhranie vytvoriť používateľa, priradiť mu oprávnenie s akými privilegovanými účtami môže disponovať a pre aké časové obdobie. Riešenie následne zašle email novému užívateľovi a umožní mu bezpečné vzdialené pripojenie k PAM riešeniu.
PIM 025	Spojenie medzi externým užívateľom a riešením PIM musí byť plne šifrované. Nie je umožnené priame spojenie medzi stanicou užívateľa a cieľovým systémom - je využitý princíp bezpečného 'jump' servera.	ÁNO	Spojenie medzi externým užívateľom a riešením PIM je plne šifrované. Nie je umožnené priame spojenie medzi stanicou užívateľa a cieľovým systémom - je využitý princíp bezpečného 'jump' servera.
PIM 026	Systém musí umožňovať audit jednotlivých akcií užívateľov s privilegovanými účtami - zobrazenie hesla, zmeny uložených údajov, vytvorenie relácie.	ÁNO	Systém umoznuje audit jednotlivých akcií užívateľov s privilegovanými účtami - zobrazenie hesla, zmeny uložených údajov, vytvorenie relácie.
PIM 027	Riešenie musí umožňovať vygenerovanie reportu všetkých aktivít administrátora riešenia.	ÁNO	Riešenie umoznuje vygenerovanie reportu všetkých aktivít administrátora riešenia.
PIM 028	Riešenie umožňuje nastavenie prístupu k reportom iba pre vybraných užívateľov.	ÁNO	Riešenie umožňuje nastavenie prístupu k reportom iba pre vybraných užívateľov.
PIM 029	Riešenie musí umožňovať nezmazateľnosť logov po dobu minimálne 30 dní. Auditné záznamy musia byť bezpečne uložené v zašifrovanej podobe, tak aby k nim mal prístup iba oprávnený užívateľ.	ÁNO	Riešenie umoznuje nezmazateľnosť logov po dobu minimálne 30 dní. Auditné záznamy su bezpečne uložené v zašifrovanej podobe, tak aby k nim mal prístup iba oprávnený užívateľ.

PIM 030	Systém musí umožňovať integráciu s nástrojmi log manager a SIEM - prenos logovaných auditných záznamov, najlepšie v reálnom čase pomocou Syslog.	ÁNO	Systém umoznuje integráciu s nástrojmi log manager a SIEM - prenos logovaných auditných záznamov, najlepšie v reálnom čase pomocou Syslog.
PIM 031	Všetky komponenty riešenia musia spĺňať nároky na vysoké zabezpečenie a automaticky vynucovať tzv. hardening. Úložisko dát, kde sú uložené jednotlivé účty, prihlasovacie údaje, nahrávky relácií a auditné záznamy, je vysoko zabezpečené a oddelené od ostatných komponentov riešenia. Databáza dát je súčasťou riešenia a nie je nutné využívať nástroje tretích strán. Táto požiadavka platí pre všetky údaje v rámci riešenia	ÁNO	Všetky komponenty riešenia spĺňajú nároky na vysoké zabezpečenie a automaticky vynucovať tzv. hardening. Úložisko dát, kde sú uložené jednotlivé účty, prihlasovacie údaje, nahrávky relácií a auditné záznamy, je vysoko zabezpečené a oddelené od ostatných komponentov riešenia. Databáza dát je súčasťou riešenia a nie je nutné využívať nástroje tretích strán.
PIM 032	Riešenie musí podporovať nasadenie vo vysokej dostupnosti a vlastné technologické možnosti (nie sú používané nástroje/SW tretích strán) pre zabezpečenie High Availability, Disaster Recovery a zálohovanie tak, aby citlivé dáta boli stále vysoko zabezpečené a dostupné iba vlastníkom dát.	ÁNO	Riešenie podporuje nasadenie vo vysokej dostupnosti a vlastné technologické možnosti (nie sú používané nástroje/SW tretích strán) pre zabezpečenie High Availability, Disaster Recovery a zálohovanie tak, aby citlivé dáta boli stále vysoko zabezpečené a dostupné iba vlastníkom dát.
PIM 033	Riešenie musí umožňovať bezpečné zálohovanie dát systému - zálohy musia byť šifrované a prístup k zálohovaným dátam je umožnený iba pomocou zabezpečených Disaster Recovery kľúčov.	ÁNO	Riešenie umožňuje bezpečné zálohovanie dát systému - zálohy sú šifrované a prístup k zálohovaným dátam je umožnený iba pomocou zabezpečených Disaster Recovery kľúčov.
PIM 034	Riešenie musí byť dimenzované minimálne pre 20 užívateľov s plným užívateľským prístupom (dostupné všetky funkcie riešenia). Licencia nie je obmedzená na počet koncových zariadení alebo riadených účtov. Súčasťou licencie je aj riešenie redundancie všetkých komponentov a taktiež geo-redundancia (aspoň active-passive) s dodatočnou miestnou redundanciou v druhej geolokácii.	ÁNO	Riešenie je dimenzované minimálne pre 20 užívateľov s plným užívateľským prístupom (dostupné všetky funkcie riešenia). Licencia nie je obmedzená na počet koncových zariadení alebo riadených účtov. Súčasťou licencie je aj riešenie redundancie všetkých komponentov a taktiež geo-redundancia (aspoň active-passive) s dodatočnou miestnou redundanciou v druhej geolokácii.
PIM 035	Licencia zároveň pokrýva možnosť inštalácie dvoch separátnych testovacích prostredí s plnou funkčnosťou a plným rozsahom.	ÁNO	Licencia zároveň pokrýva možnosť inštalácie dvoch separátnych testovacích prostredí s plnou funkčnosťou a plným rozsahom.
PIM 036	Služby: - vrátane inštalačných, konfiguračných prác a integrácie do prostredia ŠÚ SR - základné zaškolenie na dodané riešenie - upgrade a update - minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín	ÁNO	Služby: - vrátane inštalačných, konfiguračných prác a integrácie do prostredia ŠÚ SR - základné zaškolenie na dodané riešenie - upgrade a update - minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín
PIM 037	Verejný obstarávateľ upozorňuje, že dodá HW, ktorý bude vo vlastníctve ŠÚ SR, s technickými parametrami uvedenými v Prílohe č. 17 súťažných podkladov. - verejný obstarávateľ zároveň upozorňuje, že v prípade, ak sú technické parametre HW nepostačujúce pre uchádzačom navrhnuté riešenie SW, je potrebné rozširujúce komponenty HW uviesť, dodať a naceniť na vlastné náklady v rámci ponuky. Záruka minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín (platí len v prípade rozširujúcich komponentov HW)	ÁNO	HW špecifikovaný technickými parametrami uvedenými v Prílohe č.17 súťažných podkladov spĺňa predpoklady prevádzkyschopnosti nami ponúkaného PIM riešenia. Súhlasíme s parametrami dodaného HW obstarávateľom.
PIM 038	Termín dodania najneskôr do 09/2023, najskôr však po vykonaní Penetračného testovania (bod 2.4. opisu predmetu zákazky).	ÁNO	Uchádzač nevypĺňa Vlastný návrh riešenia/plnenia predmetu zákazky pri PIM 038
DLP (Data leakage prevention)			
ID	**Popis**	**Splnenie požiadaviek (áno/nie)** *vyplní uchádzač*	**Vlastný návrh riešenia/plnenia predmetu zákazky** *vyplní uchádzač*

DLP 001	Požadujeme dodanie riešenia DLP vo forme programového vybavenia pre koncové zariadenia na platforme MS Windows.	ÁNO	Safetica Enterprise DLP
DLP 002	Pred nasadením DLP riešenia na zariadenia musí dodávateľ zmapovať spôsob a formu spracovania dát pomocou modulu tzv. auditor - odkiaľ dáta prichádzajú, ako vznikajú, ako sa s nimi narába a kam putujú ďalej. Počet zariadení je 600.	ÁNO	Riesenie zmapuje tok dat.
DLP 003	Riešenie musí reportovať a blokovať aktivity ako: - operácie so súbormi - práca s elektronickou poštou a prístupom do siete Internet - využívanie aplikácií - využívanie tlačiarní (virtuálne lokálne sieťové) - práca s pevnými diskami a pamäťovými médiami všeobecne - prenos súborov po sieti	ÁNO	Riešenie reportuje a blokuje aktivity: - operácie so súbormi - práca s elektronickou poštou a prístupom do siete Internet - využívanie aplikácií - využívanie tlačiarní (virtuálne lokálne sieťové) - práca s pevnými diskami a pamäťovými médiami všeobecne - prenos súborov po sieti
DLP 004	Požadovaná je integrácia s MS AD	ÁNO	Riesenie je integrovane s MS AD.
DLP 005	Požadovaná je ochrana proti zastaveniu samotného programového vybavenia, ochrana proti odinštalovaniu služby, ochrana proti editácii registrov, systémových komponentov a knižníc. Ochrana proti zmene nastavenia a techniky na reštart a obnovu služby.	ÁNO	Riesenie poskytuje ochranu proti zastaveniu samotného programového vybavenia, ochrana proti odinštalovaniu služby, ochrana proti editácii registrov, systémových komponentov a knižníc. Ochrana proti zmene nastavenia a techniky na reštart a obnovu služby.
DLP 006	Riešenie musí zabezpečiť funkčnosť podľa prednastavených politík aj v offline móde.	ÁNO	Riešenie ma funkčnosť podľa prednastavených politík aj v offline móde.
DLP 007	Riešenie musí generovať výstrahy formou elektronickej pošty v prípade identifikovaných bezpečnostných incidentov.	ÁNO	Riešenie generuje výstrahy formou elektronickej pošty v prípade identifikovaných bezpečnostných incidentov.
DLP 008	Riešenie musí poskytnúť detailné informácie o využívaných aplikáciách, a poskytnúť kategorizáciu aplikácií.	ÁNO	Riešenie poskytuje detailné informácie o využívaných aplikáciách, a poskytnúť kategorizáciu aplikácií.
DLP 009	Riešenie musí na základe definície kategórie citlivých dát obmedziť pohyb a prácu s týmito dátami.	ÁNO	Riešenie umoznuje na základe definície kategórie citlivých dát obmedziť pohyb a prácu s týmito dátami.
DLP 010	Riešenie musí umožniť konfiguráciu politík pre vybrané aplikácie vo forme definície zdroja a cieľa užívateľských operácií.	ÁNO	Riešenie umoznuje konfiguráciu politík pre vybrané aplikácie vo forme definície zdroja a cieľa užívateľských operácií.
DLP 011	Možnosť úplne blokovať užívateľské operácie, informovať užívateľa notifikáciami, logovať užívateľské akcie.	ÁNO	Riesneie poskytuje úplne blokovať užívateľské operácie, informovať užívateľa notifikáciami, logovať užívateľské akcie.
DLP 012	Možnosť definovať citlivé dáta pomocou preddefinovaných slovníkov a algoritmov, vlastných reťazcov a regulárnych výrazov.	ÁNO	Riesenie umoznuje definovať citlivé dáta pomocou preddefinovaných slovníkov a algoritmov, vlastných reťazcov a regulárnych výrazov.
DLP 013	Možnosť importu vlastných slovníkov.	ÁNO	Možnosť importu vlastných slovníkov.
DLP 014	Dynamické reštrikcie nad súbormi a aplikáciami na základe detekovaného citlivého obsahu.	ÁNO	Dynamické reštrikcie nad súbormi a aplikáciami na základe detekovaného citlivého obsahu.
DLP 015	Blokovanie odosielania citlivých dát mimo koncovú stanicu, komunikačnými cestami ako email, web, externé zariadenie, IM.	ÁNO	Blokovanie odosielania citlivých dát mimo koncovú stanicu, komunikačnými cestami ako email, web, externé zariadenie, IM.
DLP 016	Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov.	ÁNO	Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov.
DLP 017	Podpora : - MS Windows 7, 8.1, 10 a 11 - serverových operačných systémov Windows server 2016, 2019 a 2022 - terminálových prostredí	ÁNO	Podpora : - MS Windows 7, 8.1, 10 a 11 - serverových operačných systémov Windows server 2016, 2019 a 2022 - terminálových prostredí

DLP 018	Centrálna administrátorská konzola, multitenantná administrácia v súlade s organizačným členením subjektov na úrovni domény	ÁNO	Centrálna administrátorská konzola, multitenantná administrácia v súlade s organizačným členením subjektov na úrovni domény
DLP 019	Riadené užívateľské práva do nastavení konzoly, k výsledným logom a administrácie riešenia	ÁNO	Riadené užívateľské práva do nastavení konzoly, k výsledným logom a administrácie riešenia

DLP 020	Skrytý režim na koncovej stanici vrátane procesov a zložiek, a to vrátane lokálnych a doménových administrátorov	ÁNO	Skrytý režim na koncovej stanici vrátane procesov a zložiek, a to vrátane lokálnych a doménových administrátorov
DLP 021	Služby: - vrátane inštalačných, konfiguračných prác a integrácie do prostredia ŠÚ SR - základné zaškolenie na dodané riešenie - upgrade a update - minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín	ÁNO	Služby: - vrátane inštalačných, konfiguračných prác a integrácie do prostredia ŠÚ SR - základné zaškolenie na dodané riešenie - upgrade a update - minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín
DLP 022	Verejný obstarávateľ upozorňuje, že dodá HW, ktorý bude vo vlastníctve ŠÚ SR, s technickými parametrami uvedenými v Prílohe č. 17 súťažných podkladov. - verejný obstarávateľ zároveň upozorňuje, že v prípade, ak sú technické parametre HW nepostačujúce pre uchádzačom navrhnuté riešenie SW, je potrebné rozširujúce komponenty HW uviesť, dodať a naceniť na vlastné náklady v rámci ponuky. Záruka minimálne 3 roky s podporu 24x7 s reakciou na incidenty do 24 hodín (platí len v prípade rozširujúcich komponentov HW).	ÁNO	HW špecifikovaný technickými parametrami uvedenými v Prílohe č.17 súťažných podkladov spĺňa predpoklady prevádzkyschopnosti nami ponúkaného DLP riešenia. Súhlasíme s parametrami dodaného HW obstarávateľom.
DLP 023	Termín najneskôr do 09/2023, najskôr však po vykonaní Penetračného testovania (bod 2.4. opisu predmetu zákazky).	ÁNO	Uchádzač nevypĺňa Vlastný návrh riešenia/plnenia predmetu zákazky pri DLP 023

Penetračné testovanie

ID	**Popis**	**Splnenie požiadaviek (áno/nie)** ***vyplní uchádzač***	**Vlastný návrh riešenia/plnenia predmetu zákazky** ***vyplní uchádzač***
PEN 001	Aplikačná bezpečnosť - weboveho serveru Cieľ testu je čo najdôkladnejšie a najdetailnejšie otestovať webové aplikácie a webové servre (všetky formuláre, všetky druhy známych zraniteľností).	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP • A01:2021-Broken Access Control • A02:2021-Cryptographic Failures • A03:2021-Injection • A04:2021-Insecure Design • A05:2021-Security Misconfiguration • A06:2021-Vulnerable and Outdated Components • A07:2021-Identification and Authentication Failures • A08:2021-Software and Data Integrity Failures • A09:2021-Security Logging and Monitoring Failures • A10:2021-Server-Side Request Forgery
PEN 001.1	praktická “hackerská” demonštrácia odhalených kritických zraniteľností (tvorba vlastných “exploit” programov, dump databázy, demonštrácia CSRF/XSS/Session fixation zraniteľností atď)	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu • využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, • skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 001.2	kompletné a úplné otestovanie webových aplikácií podľa testovacej príručky OWASP 30	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box

PEN 002	Sieťová bezpečnosť - externý test Test je realizovaný z pohľadu potenciálneho anonymného útočníka z Internetu, ktorý nedisponuje žiadnymi informáciami o testovanej topológii a testovaných službách.	ÁNO	Penetračné testy časti prostredia, ktoré sa netýkali webových aplikácií, vychádzali zo štandardov: • The Penetration Testing Execution Standard (PTES), • Open Source Security Testing Methodology Manual (OSSTMM).
PEN 002.1	Kontrola zraniteľností – vykonanie bezpečnostného scanu na odhalenie dostupných existujúcich zraniteľností v službách zistených počas porstcanu	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 002.2	Prienik – snaha o zneužitie dostupných zraniteľností a nedostatočnej konfigurácie za účelom prieniku do ostatných systémov a zariadení, zvýšenia užívateľských oprávnení a prístupu k prostriedkom	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 002.3	Zbieranie Informácií – o cieľovom systéme sú zozbierané, identifikované a analyzované všetky informácie, vrátane verzie webového serveru, použitých modulov, programovej platformy, WAF a prístupových bodov do aplikácie	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 002.4	Enumerovanie a mapovanie zraniteľností – pomocou intruzívnych metód a techník (špeciálne skonštruované HTTP žiadosti) sú identifikované potenciálne slabiny (použité sú špeciálne bezpečnostné scannery, “fault-injection proxies” ako aj manuálne overenie)	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 002.5	Využitie zraniteľností – pokus o získanie prístupu pomocou zraniteľností identifikovaných v predchádzajúcej fáze. Cieľom je získať používateľský alebo privilegovaný (administrátorsky) prístup do aplikácie alebo operačného systému (použité sú špeciálne “exploit” skripty a “exploit” systémy	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 002.6	Testovanie poštového serveru – okrem testovania známych zraniteľností v konkrétnej implementácii MTA servera, je realizovaných niekoľko detailných SMTP testov na overenie „relaying problémov” MTA servera, takže sú odhalené všetky možnosti zneužitia SMTP servera prípadným spamerom a odolnosti MTA servera na potenciálny DOS útok. Test sa vzťahuje na všetky MX servery pre danú testovanú doménu. Súčasne sú otestované potenciálne zneužiteľné zraniteľnosti antivírových a antispamových implementácií.	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 002.7	Testovanie DNS zón – okrem testovania známych zraniteľností v konkrétnej implementácii DNS servera (Bind, Microsoft DNS server) je realizovaný tiež test konzistencie zón na všetkých zadaných DNS serveroch, kontrola možnosti verejného „zone transfer”, zraniteľnosť na DNS „caching” útoky atď. Súčasne sú realizované detailné penetračné testy každého DNS servera pre danú doménu (aj mimo siete objednávateľa – v tomto prípade je nutný ale súhlas príslušného prevádzkovateľa).	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.

PEN 003	Sieťová bezpečnosť - interný test Test je realizovaný z pohľadu potenciálneho anonymného útočníka z vnútra organizácie, ktorý nedisponuje žiadnymi informáciami o testovanej topológii a testovaných službách.	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 003.1	Kontrola zraniteľností – vykonanie bezpečnostného skenu na odhalenie dostupných existujúcich zraniteľností v službách zistených počas portscanu	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 003.2	Prienik – snaha o zneužitie dostupných zraniteľností a nedostatočnej konfigurácie za účelom prieniku do ostatných systémov a zariadení, zvýšenia užívateľských oprávnení a prístupu k prostriedkom	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 003.3	Zbieranie Informácií – o cieľovom systéme sú zozbierané, identifikované a analyzované všetky informácie, vrátane verzie webového serveru, použitých modulov, programovej platformy, WAF a prístupových bodov do aplikácie	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 003.4	Enumerácia a mapovanie zraniteľností – pomocou intruzívnych metód a techník (špeciálne skonštruované HTTP žiadosti) sú identifikované potenciálne slabiny (použité sú špeciálne bezpečnostné scannery, “fault-injection proxies” ako aj manuálne overenie)	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 003.5	Využitie zraniteľností – pokus o získanie prístupu pomocou zraniteľností identifikovaných v predchádzajúcej fáze. Cieľom je získať používateľský alebo privilegovaný (administrátorsky) prístup do aplikácie alebo operačného systému (použité sú špeciálne “exploit” skripty a “exploit” systémy technická výsledná správa s manažérskym zhrnutím, so všetkými odhalenými zraniteľnostami, ich stupňami rizík a odporučeniami	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 004	Vulnerability sken datacentra - cloud services	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 004.1	vulnerability internal sken datacentra(jedna lokalita) - cloud services	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 004.2	inštalácia sondy, zber údajov, vyhodnotenie, report.	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.

PEN 005	Sociálne inžinierstvo	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 005.1	fyzický prienik do budovy (príprava + realizácia)	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 005.2	plošná phishingová kampaň	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 005.3	spearphishing (10 zamestnancov ŠÚ SR)	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 005.4	telefonický socialing	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 005.5	USB/keyloggers (príprava + rozmiestenie na 3 lokality)	ÁNO	využitie PTES štandardu v rozsahu pasívnej a aktívnej inteligencie minimálne v rozsahu •využitie voľne dostupných databáz pre získanie údajov o cieľovej IP adrese, •skenovanie cieľovej IP adresy za účelom identifikácie otvorených portov a aplikácií.
PEN 006	Penetračné testovanie je akceptované ako celok – t. j. musia byť vykonané všetky druhy uvedených penetračných testov.	ÁNO	Penetračné testy bodú primárne realizované na základe štandardu OWASP s ohľadom na predchádzajúce znalosti predmetného prostredia, resp. aplikácií, tzv. Grey Box
PEN 007	Penetračné testovanie je nutné realizovať pred nasadením riešení (log manager, PIM, DLP) – najneskôr však do 3 mesiacov od účinnosti zmluvy.	ÁNO	Uchádzač nevyplňa Vlastný návrh riešenia/plnenia predmetu zákazky pri PEN 007

Príloha č. 3: Zoznam subdodávateľov

Uchádzač/skupina dodávateľov:

SOITRON, s.r.o.

Plynárenská 5, 829 75 Bratislava

IČO: 35955678

Dolu podpísaný zástupca uchádzača týmto čestne vyhlasujem, že na realizácii predmetu zákazky **„Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS“** vyhlásenej verejným obstarávateľom Štatistický úrad Slovenskej republiky so sídlom Lamačská cesta 3/C, 840 05 Bratislava 45, v Úradnom vestníku Európskej únie dňa 30.01.2023 pod značkou 2023/S 021-059301 a vo Vestníku verejného obstarávania č. 22/2023 zo dňa 31.01.2023 pod značkou 3769-MSS:

☒ sa nebudú podieľať subdodávatelia a celý predmet uskutočníme vlastnými kapacitami.

☐ sa budú podieľať nasledovný subdodávatelia :

P. č.	Obchodné meno a sídlo subdodávateľa	IČO	Údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia	Podiel na realizácii zákazky v %	Predmet subdodávky
1					
2					
3					

V Bratislave, dňa .....

.....

Ing. Marián Skákala

výkonný riaditeľ a konateľ spoločnosti

SOITRON, s.r.o.

Príloha č. 4: Zoznam kľúčových expertov

Navrhovaná pozícia kľúčového experta	Meno a priezvisko	Identifikačné údaje o zamestnávateľovi kľúčového experta
Projektový manažér	Ing. Veronika Kvetáková	SOITRON, s.r.o., Plynárenská 5, 829 75 Bratislava, IČO: 35955678
Bezpečnostný architekt riešenia	Ing. Štefan Porubčan,	SOITRON, s.r.o., Plynárenská 5, 829 75 Bratislava, IČO: 35955678
Expert na implementáciu log manažmentu a SIEM	Matej Pilko	SOITRON, s.r.o., Plynárenská 5, 829 75 Bratislava, IČO: 35955678
Expert na implementáciu PIM	Michal Mašek	SOITRON, s.r.o., Plynárenská 5, 829 75 Bratislava, IČO: 35955678
Expert na implementáciu DLP	Ing. Marek Cisár	SOITRON, s.r.o., Plynárenská 5, 829 75 Bratislava, IČO: 35955678

V Bratislave, dňa .....

.....

Ing. Marián Skákala

výkonný riaditeľ a konateľ spoločnosti

SOITRON, s.r.o.

Príloha č. 5: Záväzný štruktúrovaný rozpočet ceny

Uchádzač / skupina dodávateľov	**SOITRON, s.r.o.** **Plynárenská 5, 829 75 Bratislava** **IČO: 35955678**
Kritérium na vyhodnotenie ponúk	NAJNIŽŠIA CENA V EUR S DPH
Je uchádzač platiteľom DPH?	ÁNO / ~~NIE~~

Por. č.	Názov	MJ	Cena za 1 MJ v eur bez DPH	Celková cena v eur bez DPH	DPH v eur	Celková cena v eur s DPH
1.	Log manager License + HW (LOG 001 - LOG 018)	1	55 000,00	55 000,00	11 000,00	66 000,00
2.	PIM License per USER (PIM 001 - PIM 038)	20	2 550,00	51 000,00	10 200,00	61 200,00
3.	DLP License per USER (DLP 001 - DLP 023)	600	225,00	135 000,00	27 000,00	162 000,00
4.	Penetračné testovanie (PEN 001 - PEN 007)	1	99 900,00	99 900,00	19 980,00	119 880,00
CELKOM				**340 900,00**		**409 080,00**

V Bratislave, dňa.....

.....

Ing. Marián Skákala

výkonný riaditeľ a konateľ spoločnosti

SOITRON, s.r.o.

Príloha č. 6: Všeobecné podmienky pre zabezpečenie informačnej a kybernetickej bezpečnosti Štatistického úradu Slovenskej republiky

Časť A.

Článok 1
Úvodné ustanovenia

1.1. Tieto Všeobecné podmienky, pre zabezpečenie informačnej a kybernetickej bezpečnosti (ďalej len „všeobecné podmienky“) Štatistického úradu Slovenskej republiky (ďalej len „ŠÚ SR“) stanovujú povinnosti tretej strany, ak predmet plnenia Zmluvy uzatvorenej medzi treťou stranou a Štatistickým úradom Slovenskej republiky súvisí s informačno-komunikačnými technológiami ŠÚ SR (ďalej len „IKT ŠÚ SR“).

1.2. Na účely tohto dokumentu

a) **aktívum** je všetko, čo má pre ŠÚ SR hodnotu (fyzické komponenty, softvér, dáta, služby, ľudské zdroje, povesť ŠÚ SR, ...),
b) **informácie sú** databázy a dátové súbory, zmluvy a dohody, systémová dokumentácia, informácie z výskumu, používateľské príručky, školiaci materiál, prevádzkové a podporné procedúry, plány zachovania kontinuity činnosti, záložné dohody, auditné záznamy a archivované informácie.
c) **bezpečnostným incidentom** je akýkoľvek spôsob narušenia bezpečnosti IKT, ako aj akékoľvek porušenie bezpečnostnej politiky a súvisiacich pravidiel,
d) **dostupnosť** je vlastnosť, že autorizovaní užívatelia majú v prípade požiadavky prístup k informáciám a aktívam,
e) **dôvernosť** je vlastnosť, že informácia nie je dostupná alebo prístupná neautorizovaným jednotlivcom, entitám alebo procesom,
f) **integrita** je vlastnosť, že informácie a metódy ich spracovania sú presné a kompletné,
g) **externý prístup** je prístup tretích strán, ako i interných zamestnancov ŠÚ SR,
h) **externým subjektom** je právnická osoba a štatutárom právnickej osoby určené fyzické osoby (ďalej len „zamestnanci externého subjektu“), ktoré nie sú zamestnancami ŠÚ SR a ktoré poskytujú ŠÚ SR plnenie v zmysle platných zmlúv, podľa ktorých môžu požiadať o prístup k IKT v presne určenom nevyhnutnom rozsahu,
i) **externým prístupom zamestnanca ŠÚ SR k IKT** je iný prístup zamestnanca ŠÚ SR k IKT, ako prístup zo štandardného pracoviska ŠÚ SR s LAN/WAN prepojením,
j) **externým prístupom zamestnancov externého subjektu** k IKT je prístup zamestnanca externého subjektu k IKT,
k) **IKT** sú informačno-komunikačné technológie,
l) **IKT ŠÚ SR** je súhrn nasledovných komponentov používaných na prípravu a spracovanie dát a na manažovanie informácií a procesov v ŠÚ SR:
    1. servery, pracovné stanice, faxy a príslušná dokumentácia,
    2. informačné systémy ŠÚ SR (aplikačné programové vybavenie a jeho vrstvy, ako napr. aplikačné servery, databázové servery) a príslušná dokumentácia,
    3. dáta a informácie spracovávané v informačných systémoch ŠÚ SR,
    4. zariadenia diskových polí, SAN infraštruktúra, zálohovacie zariadenia a príslušná dokumentácia,
    5. sieťová infraštruktúra a sieťové komponenty (napr. smerovače, firewally) a príslušná dokumentácia
    6. písomné záznamy súvisiace s IS ŠÚ SR.

m) **IP adresa** je adresa zariadenia pripojeného do počítačovej siete, definovaná na základe Internet Protokolu,
n) **informačné aktívum** je aktívum informačného charakteru, primárne informácie a údaje, resp. všetko ostatné, čo plní istú funkciu v procese spracovávania alebo ochrany informácií, resp. údajov,
o) **informačná a kybernetická bezpečnosť** je súbor aspektov týkajúcich sa dosiahnutia a udržiavania dôvernosti, integrity a dostupnosti informačných aktív,
p) **IS/informačný systém** je súbor činností, ktoré zabezpečujú zber, prenos, spracovanie, uloženie, výber, distribúciu a prezentáciu informácií a dát (vrátane dát v papierovej podobe) pre potreby rozhodovania tak, aby riadiaci pracovníci mohli vykonávať funkcie riadenia vo všetkých zložkách systému riadenia,
q) **LAN/WAN** je štandardná lokálna počítačová sieť a prepojenie komunikačných sietí pracovísk ŠÚ SR realizované spravidla technológiou MPLS
r) **organizačným útvarom** sú organizačné útvary ŠÚ SR,
s) **oprávnená osoba** sú všetci zamestnanci sekcie informatiky ŠÚ SR, prípadne iný zamestnanec písomne poverený riaditeľom sekcie informačných systémov, alebo manažérom informačnej a kybernetickej bezpečnosti, na výkon úloh vyplývajúcich z činností spojených s tretími stranami a s externými prístupmi interných zamestnancov,
t) **outsourcing alebo subzhotoviteľ** je zabezpečenie podporných služieb externou organizáciou,
u) **používateľom externého prístupu** je zamestnanec ŠÚ SR alebo zamestnanec externého subjektu, ktorému bol povolený externý prístup k IKT,
v) **prístup tretej strany k IKT ŠÚ SR** je prístup tretej strany k hardvéru alebo softvéru alebo dátam IKT ŠÚ SR , vrátane príslušnej dokumentácie,
w) **tretie strany** sú externí dodávatelia a externí odberatelia vybraných služieb ŠÚ SR. V tejto súvislosti ide predovšetkým o externé subjekty, ktoré na zmluvnom základe s ŠÚ SR dodávajú pre ŠÚ SR alebo odoberajú od ŠÚ SR špecializované údaje alebo vykonávajú pre ŠÚ SR špecializované práce súvisiace s návrhom, implementáciou, testovaním, dodávaním, údržbou, aktualizáciou alebo outsorucingom IKT, ako aj o ich subzhotoviteľov,
x) **VPN kanál** je bezpečnostný kanál, ktorý vytvára šifrované spojenie na pripojenie tretej strany k IKT ŠÚ SR na základe Virtual Private Network techník,
y) **vzdialený prístup** je prístup tretej strany k softvéru alebo dátam IKT ŠÚ SR z iného miesta ako z priestorov ŠÚ SR,

Článok 2
Základné požiadavky

2.1. Zhotoviteľ sa zaväzuje oboznámiť svojich zamestnancov zúčastňujúcich sa na predmete plnenia Zmluvy s bezpečnostnými požiadavkami v rozsahu uvedenom v týchto všeobecných podmienkach pre zabezpečenie informačnej a kybernetickej bezpečnosti ŠÚ SR.

2.2. Zhotoviteľ sa zaväzuje oboznámiť a následne zabezpečiť od svojich zamestnancov, realizujúcich predmet plnenia Zmluvy, dodržiavanie týchto povinností:
a) dodržiavať ochranu údajov a informácií súvisiacich s IKT a s existujúcimi alebo vyvíjanými informačnými systémami ŠÚ SR a záväzok mlčanlivosti o údajoch a informáciách, s ktorými počas výkonu prác vo ŠÚ SR prišli do styku, ako aj zákaz ich využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní, a to aj po ukončení pracovného, resp. zmluvného pomeru,
b) zachovávať daňové tajomstvo, s ktorým počas výkonu prác v ŠÚ SR prišli do styku, ako aj zákaz jeho využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní a to aj po ukončení pracovného pomeru, resp. zmluvného pomeru,

c) zachovávať mlčanlivosť o osobných údajoch, s ktorými počas výkonu prác v ŠÚ SR prišli do styku, ako aj zákaz ich využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní a vo vzťahu k Úradu pre ochranu osobných údajov pri plnení jeho úloh,
d) preukázať na vyzvanie svoju totožnosť, buď zamestnancom strážnej služby alebo Oprávnenej osobe určenej na priamu komunikáciu s ním pri vstupe do priestorov ŠÚ SR,
e) realizovať zásahy do IKT ŠÚ SR iba v určenom rozsahu v rámci plnenia Zmluvy a poskytovania dohodnutých prác pre ŠÚ SR,
f) použiť externé pripojenia k IKT ŠÚ SR len spôsobom, ktorý nie je v rozpore so všeobecne záväznými právnymi predpismi a bezpečnostnými politikami ŠÚ SR,
g) používať externé pripojenia k IKT ŠÚ SR výhradne na plnenie povinností v zmysle platnej Zmluvy uzatvorenej s cieľom poskytnutia plnenia podľa Zmluvy externého subjektu v prospech ŠÚ SR,
h) neposkytnúť svoju elektronickú identitu (napr. login, heslo, a pod.) inej osobe,
i) realizovať výkon plnenia Zmluvy tak, aby pri ňom nedošlo k poškodeniu alebo zničeniu kľúčových komponentov IKT alebo k neočakávanému prerušeniu ich prevádzky,
j) riadiť sa pokynmi Oprávnenej osoby, riaditeľa sekcie informačných systémov, SLA manažéra ŠÚ SR, manažéra informačnej a kybernetickej bezpečnosti, riaditeľa IKT ŠÚ SR počas výkonu plnenia Zmluvy pre ŠÚ SR,
k) zdokumentovať všetky zásahy do IKT ŠÚ SR podľa pokynov Oprávnenej osoby a bezodkladne jej ohlásiť zistené bezpečnostné nedostatky, ktoré by mohli spôsobiť ohrozenie dôvernosti alebo integrity kódu alebo dokumentácie systému,
l) pripájať svoje technologické prostriedky (napr. počítač, notebook, meracie prístroje a pod.) k IKT ŠÚ SR len po predchádzajúcom súhlase Oprávnenej osoby, a to len na nevyhnutne potrebnú dobu a s rešpektovaním podmienok spojených so súhlasom, ako napríklad antivírusová kontrola a podobne,
m) možnosti vynášať zariadenia, materiál a údaje patriace ŠÚ SR (informačno-komunikačné zariadenia, výsledky zostáv vytvorených na základe skriptov, zbery údajov, poskytované údaje, a pod.) z priestorov ŠÚ SR len s písomným súhlasom Oprávnenej osoby, pričom zdokumentovaná e-mailová komunikácia je v odôvodnených a naliehavých prípadoch považovaná za súhlas Oprávnenej osoby na priamu komunikáciu so žiadateľom, ak nie je dohodnuté v Zmluve inak,
n) rešpektovať autorské práva k materiálom poskytnutým z ŠÚ SR, na ktoré bol Zhotoviteľ upozornený;
o) vrátiť všetky materiály a údaje, vrátane elektronických, poskytnuté z ŠÚ SR a zlikvidovať všetky ich kópie, ak to nebolo zmluvne dohodnuté inak.

2.3. V prípade, že predmet plnenia Zmluvy súvisí s vývojom a aktualizáciou IKT ŠÚ SR, Zhotoviteľ akceptuje nasledujúce požiadavky:
a) dodržiavanie bezpečnostných požiadaviek relevantných vnútorných predpisov ŠÚ SR, bezpečnostných politík ŠÚ SR, platnej bezpečnostnej legislatívy (najmä požiadaviek zákona o ITVS, zákona o KB), zachovávania mlčanlivosti o skutočnostiach zistených počas vývoja, nasadzovania a podpory vyvíjaného alebo aktualizovaného IS, zachovávanie mlčanlivosti podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, nevnesenie nepožadovaného kódu a nepožadovaných funkcií do IS, ktoré by mohli viesť k zneužitiu IS neautorizovanými prístupmi a osobami,
b) zabezpečenie ochrany dôvernosti, integrity a dostupnosti kódu a dokumentácie predmetu Zmluvy (do kontaktu s kódom a dokumentáciou predmetu Zmluvy ŠÚ SR umožní prichádzať iba tým zamestnancom tretej strany a osobám v obdobnom vzťahu k tretej strane ako je pracovnoprávny vzťah, ktorí podpísali Poučenie zamestnancov externého subjektu o

informačnej a kybernetickej bezpečnosti v prostredí IKT ŠÚ SR podľa časti B. tejto prílohy (ďalej len „poučenie“),

c) právo ŠÚ SR vykonať audit vývojového prostredia - účelom tohto auditu je súlad vývoja s deklarovanou metodikou, resp. normou, a dodržiavanie bezpečnostných požiadaviek,
d) zabezpečenie, aby predmet plnenia Zmluvy obsahoval aj bezpečnostné požiadavky pre vyvíjaný alebo aktualizovaný IS ,
e) vykonanie testovania pre činnosti súvisiace s bezpečnostnými požiadavkami súvisiacimi s vyvíjaným alebo aktualizovaným IS,
f) dodanie dokumentácie pre nové alebo aktualizované IKT alebo ich časti, ktorá obsahuje:
    1. používateľskú dokumentáciu, ktorou je návod na používanie predmetu Zmluvy, scenáre činností predmetu Zmluvy pre jednotlivé roly, pravidlá používania predmetu Zmluvy, opis bezpečnostných procedúr a ovládanie bezpečnostných mechanizmov, opis chybových hlásení,
    2. prevádzkovú a administrátorskú dokumentáciu, ktorou je dokumentácia o architektúre predmetu Zmluvy alebo jeho časti, popis prevádzkových postupov, postupy zotavenia sa z bežných chýb, rozdelenie rolí pri prevádzke a administrácii predmetu Zmluvy, opis konfigurácie predmetu Zmluvy a umiestnenia jednotlivých fyzických, aplikačných a dátových komponentov, väzby na existujúce informačné systémy, politiku použitia kryptografických opatrení, podrobný opis aktivít vyžadovaných pri administrácii predmetu Zmluvy, šablóny administrátorských a operátorských denníkov a uvedenie typov udalostí, ktoré sa do nich zapisujú.

2.4. Nesplnenie týchto bezpečnostných požiadaviek bude dôvodom na neukončenie príslušnej etapy projektu alebo neschválenie prevzatia vykonávaného plnenia Zmluvy.

2.5. V prípade, že predmet plnenia Zmluvy sa priamo dotýka prístupu k IKT ŠÚ SR, Zhotoviteľ okrem požiadaviek uvedených v článku 2.2. a 2.3. tejto prílohy akceptuje nasledujúce doplňujúce požiadavky:

a) zabezpečí realizovanie prístupu k softvéru alebo dátam IKT ŠÚ SR na základe žiadosti o prístup externého subjektu k IKT ŠÚ SR (ďalej len „žiadosť“). V žiadosti musí byť uvedený dôvod prístupu, rozsah prístupu (časť IKT, resp. IS, ku ktorému je požadovaný prístup), miesto prístupu a IP adresa zariadenia na prístup (v prípade vzdialeného prístupu), stanovený dátum a čas prístupu a mená zamestnancov tretej strany, pre ktorých je požadovaný prístup. Záležitosti súvisiace so žiadosťou sa realizujú prostredníctvom kontaktných osôb a oprávnených zamestnancov. Žiadosť Zhotoviteľa o prístup k IKT ŠÚ SR podpísaná kontaktnou osobou za Zhotoviteľa, sa elektronicky (spolu so žiadosťou), poštou alebo osobne doručí kontaktnej osobe ŠÚ SR.

   Kontaktná osoba ŠÚ SR doručí schválený resp. neschválený súhlas s prístupom k IKT ŠÚ SR elektronicky, poštou alebo osobne kontaktnej osobe Zhotoviteľa.
b) zabezpečí, aby všetci jeho zamestnanci realizujúci prístup k IKT ŠÚ SR na základe pokynov kontaktnej osoby ŠÚ SR alebo Oprávneného zamestnanca podpísali pred prvým prístupom k IKT ŠÚ SR poučenie. V prípade odmietnutia podpísania tohto poučenia, nebude príslušnému zamestnancovi umožnený prístup k IKT ŠÚ SR,
c) zabezpečí, aby všetky zásahy jeho zamestnancov do IKT ŠÚ SR boli zaznamenané v protokole z prístupu tretích strán k IKT ŠÚ SR. Mesačný výpis bude dodaný raz mesačne vždy do 15 dňa nasledujúceho mesiaca po mesiaci realizácie zásahu.

Článok 3
Záverečné ustanovenia

3.1. Všeobecné podmienky sú záväzné pre Zhotoviteľa v plnom rozsahu pokiaľ v Zmluve nie je ustanovené inak.

Časť B.

Poučenie zamestnancov externého subjektu o informačnej a kybernetickej bezpečnosti v prostredí IKT ŠÚ SR

V zmysle relevantných vnútorných predpisov Štatistického úradu Slovenskej republiky (ďalej len „ŠÚ SR“), týkajúcich sa prístupu externých subjektov k informačným a komunikačným technológiám (ďalej len „IKT“) ŠÚ SR, bezpečnostných politík ŠÚ SR, platnej bezpečnostnej legislatívy (najmä požiadaviek zákona č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov), mlčanlivosti v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zamestnanec tretej strany má tieto povinnosti:

a) dodržiavať ochranu údajov a informácií súvisiacich s IKT a s existujúcimi alebo vyvíjanými informačnými systémami ŠÚ SR (ďalej aj „predmetom plnenia Zmluvy“) a záväzok mlčanlivosti o údajoch a informáciách, s ktorými počas výkonu prác v ŠÚ SR príde do styku, ako aj zákaz ich využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní, a to aj po ukončení pracovného, resp. zmluvného pomeru,
b) zachovávať mlčanlivosť o osobných údajoch, s ktorými počas výkonu prác v ŠÚ SR prišiel do styku, ako aj zákaz ich využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní a vo vzťahu k Úradu pre ochranu osobných údajov pri plnení jeho úloh,
c) preukázať na vyzvanie svoju totožnosť, buď zamestnancom strážnej služby alebo Oprávnenej osoby určenej na priamu komunikáciu s ním pri vstupe do priestorov ŠÚ SR,
d) realizovať zásahy do IKT ŠÚ SR iba v určenom rozsahu v rámci poskytovania dohodnutých prác a služieb pre ŠÚ SR,
e) použiť len také externé pripojenia k IKT ŠÚ SR, ktoré sú uvedené v písomnej žiadosti o prístup externého subjektu k IKT ŠÚ SR,
f) použiť externé pripojenia k IKT ŠÚ SR len spôsobom, ktorý nie je v rozpore so všeobecne záväznými právnymi predpismi a bezpečnostnými politikami ŠÚ SR,
g) používať externé pripojenia k IKT ŠÚ SR výhradne na plnenie povinností, v zmysle platnej Zmluvy,
h) neposkytnúť svoju elektronickú identitu (napr. login, heslo, a pod.) inej osobe,
i) realizovať výkon dohodnutých prác a služieb tak, aby pri nich nedošlo k poškodeniu alebo zničeniu kľúčových komponentov IKT alebo k neočakávanému prerušeniu ich prevádzky,
j) riadiť sa pokynmi SLA manažéra ŠÚ SR, manažéra informačnej a kybernetickej bezpečnosti, riaditeľa odboru IKT, riaditeľa sekcie informačných systémov ŠÚ SR (ďalej aj ako „Oprávnená osoba“) počas výkonu dohodnutých prác a služieb pre ŠÚ SR,
k) zdokumentovať všetky zásahy do IKT ŠÚ SR podľa pokynov Oprávnenej osoby a bezodkladne jej ohlásiť zistené bezpečnostné nedostatky, ktoré by mohli spôsobiť ohrozenie dôvernosti alebo integrity kódu alebo dokumentácie predmetu Zmluvy,
l) pripájať svoje technologické prostriedky (napr. počítač, notebook, meracie prístroje a pod.) k IKT ŠÚ SR len po predchádzajúcom súhlase Oprávnenej osoby, a to len na nevyhnutne potrebnú dobu a s rešpektovaním podmienok spojených so súhlasom, ako napríklad antivírusová kontrola a podobne,
m) možnosti vynášať zariadenia, materiál a údaje patriace ŠÚ SR (informačno-komunikačné zariadenia, výsledky zostáv vytvorených na základe skriptov, zbery údajov, poskytované údaje, a pod.) z priestorov ŠÚ SR, len s písomným súhlasom Oprávnenej osoby, pričom zdokumentovaná e-mailová komunikácia je v odôvodnených a naliehavých prípadoch považovaná za súhlas Oprávnenej osoby na priamu komunikáciu so žiadateľom,
n) rešpektovať autorské práva k materiálom poskytnutým zo ŠÚ SR, na ktoré bola Zhotoviteľ upozornená,

o) vrátiť všetky materiály a údaje, vrátane elektronických, poskytnuté z ŠÚ SR a zlikvidovať všetky ich kópie, ak to nebolo zmluvne dohodnuté inak.

Svojím vlastnoručným podpisom potvrdzujem, že som tomuto poučeniu v plnom rozsahu porozumel, nemám voči nemu žiadne výhrady a zaväzujem sa ho dodržiavať.

P.č.	Titul, meno, priezvisko	Číslo OP	Funkcia	Názov právnickej osoby/SZČO	Dátum	Podpis