

## Smlouva o zajištění podpory provozu a maintenance DLP Software Safetica One Enterprise

uzavřená v souladu s ustanoveními § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném a účinném znění (dále jen „Smlouva“)

mezi:

**Objednatel:** ČR - Státní úřad inspekce práce  
Se sídlem: Kolářská 451/13, 746 01 Opava  
IČ: 750 46 962  
Jednající/zast.: Mgr. Ing. Rudolf Hahn, generální inspektor SÚIP  
Bankovní spojení: Česká národní banka  
Číslo účtu: ██████████  
datová schránka: cmwaazf

(dále jen „Objednatel“) na straně jedné

a

**Poskytovatelem:** Safetica a.s.  
Se sídlem: Laubova 1729/8, 130 00 Praha 3  
IČ: 258 48 666  
DIČ: CZ25848666  
Jednající/zast.: Ing. Richard Brulík, člen představenstva  
Bankovní spojení: ██████████  
č. účtu: ██████████  
Plátce DPH: ano  
Datová schránka: d76wexq

Zapsán v obchodním rejstříku vedeném Městským soudem v Praze pod sp. Zn. B 27205

(dále jen „Poskytovatel“) na straně druhé

(dále společně také „smluvní strany“)

### Preambule

1. Předmětem Smlouvy je dvoustranný právní vztah mezi smluvními stranami, jehož obsahem jsou práva a povinnosti související s realizací veřejné zakázky malého rozsahu na služby s názvem „VZMR č. 07/23 – SÚIP – Prodloužení maintenance DLP Software Safetica One Enterprise o 4 roky“.
2. Tuto smlouvu uzavřely smluvní strany na základě úplného konsensu o níže uvedených ustanoveních, v souladu s příslušnými ustanoveními obecně závazných právních předpisů, a to zejména zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), zákona č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů (dále jen „autorský zákon“) a licenční smlouvy s koncovým uživatelem počítačového programu „Licenční podmínky Safetica“ (dále jen „End User License Agreement“ nebo také jako „smlouva EULA“).
3. V otázkách týkajících se výkladu Smlouvy, má Smlouva přednost před zadávací dokumentací, zadávací dokumentace má přednost před nabídkou, nikoliv však před kogentními ustanoveními

občanského zákoníku a ostatních obecně závazných právních předpisů. Dokumenty výše uvedené v čl. 3 Preambule mají přednost před smlouvou EULA.

4. Objednatel prohlašuje, že má licenci Safetica One Enterprise v rozsahu uvedeném v příloze č. 1 Smlouvy, kdy tato příloha definovala předmět plnění smlouvy o dílo uzavřené dne 21. 10. 2021 mezi Objednatel a Zhotovitelem, tj. Safetica Technologies s.r.o., Laubova 1729/8, 130 00 Praha – Vinohrady, IČ: 258 48 666.
5. Poskytovatel prohlašuje, že má zákonem vyžadovanou odbornou způsobilost pro splnění předmětu Smlouvy, kterou doložil v nabídce. Způsobilost Poskytovatele musí trvat po celou dobu trvání Smlouvy.

## **1. Předmět Smlouvy**

- 1.1 Předmětem Smlouvy je prodloužení maintenance DLP software Safetica One Enterprise (dále jen „systém DLP“) o 4 roky, včetně implementace a registrace (dále jen „služby“ nebo „plnění“) dle technické specifikace, která byla součástí nabídky účastníka a je přílohou č. 2 Smlouvy - Technická specifikace a kalkulace nabídkové ceny plnění.
- 1.2 Součástí plnění je rovněž zpracování dalších souvisejících dokumentů v rozsahu uvedeném v příloze č. 2 Smlouvy.
- 1.3 Služba musí být poskytována v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB“) včetně požadavků plynoucích z jeho prováděcí vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „VKB“).

## **2. Platnost a účinnost Smlouvy**

- 2.1 Smlouva nabývá platnosti dnem jejího podpisu poslední smluvní stranou.
- 2.2 Smlouva nabývá účinnosti dnem uveřejnění v registru smluv, dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „zákon o registru smluv“).
- 2.3 Poskytovatel bere na vědomí, že na Smlouvu dopadá povinnost uveřejnění v registru smluv dle zákona o registru smluv. Zveřejnění v registru smluv zajistí Objednatel, který se současně zavazuje informovat Poskytovatele o provedení registrace tak, že zašle potvrzení správce Registru smluv o uveřejnění Smlouvy bez zbytečného odkladu poté, kdy sám potvrzení obdrží, popř. již v průvodním formuláři vyplní příslušnou kolonku s ID datové schránky Poskytovatele (v takovém případě potvrzení od správce registru smluv o provedení registrace Smlouvy obdrží obě smluvní strany zároveň).

## **3. Termín plnění, doba trvání Smlouvy, dodací podmínky**

- 3.1 Termín zahájení plnění je ode dne 22. 12. 2023.
- 3.2 V případě, že Poskytovatel do data uvedeného v čl. 3.1 Smlouvy plnění nezačíná, a to včetně předání faktury, je Objednatel oprávněn od Smlouvy odstoupit.
- 3.3 Smlouva se uzavírá na dobu určitou, a to na dobu 4 let od termínu zahájení plnění dle čl. 3.1 Smlouvy.

- 3.4 Místem plnění je sídlo Objednatele, tj.: Státní úřad inspekce práce, Kolářská 451/13, 746 01 Opava.

#### **4. Skončení Smlouvy, výpověď a odstoupení**

- 4.1 Platnost Smlouvy lze ukončit písemnou dohodou podepsanou oprávněnými zástupci obou smluvních stran.
- 4.2 Objednatel může od Smlouvy odstoupit, pokud Poskytovatel nezahájí plnění v termínu nebo kvalitě dle Smlouvy.
- 4.3 Poskytovatel může od Smlouvy odstoupit, pokud Objednatel nezaplatí cenu za řádně zahájené plnění dle Smlouvy.
- 4.4 Odstoupení nabývá účinnosti dnem následujícím po dni prokazatelného doručení jeho písemného vyhotovení druhé smluvní straně.
- 4.5 V případě ukončení Smlouvy z důvodu uvedeného v čl. 4.2 Smlouvy je Poskytovatel povinen vrátit alikvotní část uhrazených finančních prostředků dle čl. 5.2 Smlouvy, a to počítanou jako poměr počtu kalendářních dnů, kdy byly služby poskytovány k počtu kalendářních dnů, kdy poskytovány nebudou, tedy ode dne nabytí účinnosti odstoupení dle čl. 4.4 Smlouvy.
- 4.6 Objednatel je oprávněn ukončit tuto Smlouvu i písemnou výpovědí bez udání důvodu, a to ve lhůtě do 1. 10. daného roku, v takovém případě bude smluvní vztah mezi Objednatelem a Poskytovatelem výpovědí ukončen k 21.12. daného roku, tedy plnění dle Smlouvy bude Poskytovatelem poskytováno až do 21.12. daného roku včetně.
- 4.7 Zánikem Smlouvy nejsou nikterak dotčena práva smluvních stran na smluvní pokuty, náhradu škody či jiné peněžité nároky, splatné přede dnem zániku Smlouvy.
- 4.8 Odstoupení smluvní strany či návrh dohody lze druhé smluvní straně zaslat prostřednictvím poskytovatele poštovních služeb nebo způsobem uvedeným v čl. 13.1 Smlouvy.

#### **5. Cena a platební podmínky**

- 5.1 Cena předmětu Smlouvy je stanovena v příloze č. 2 Smlouvy – Technická specifikace a kalkulace nabídkové ceny plnění, jež je nedílnou součástí Smlouvy. Tato cena obsahuje veškeré náklady spojené s plněním předmětu Smlouvy. Případné více náklady nejsou přípustné. Objednatel nepřipouští překročení níže uvedené ceny vyjma změny sazeb DPH a jen o vyšší změny této sazby DPH.
- 5.2 Platba bude probíhat výhradně v Kč (CZK), rovněž veškeré cenové údaje budou v této měně.
- 5.3 Cena za celé plnění dle Smlouvy bude Objednatelem uhrazena na základě daňového dokladu – faktury Poskytovatele – na účet Poskytovatele uvedený v záhlaví Smlouvy. Faktura musí obsahovat všechny náležitosti řádného účetního a daňového dokladu ve smyslu příslušných právních předpisů (zejména zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, ZoDPH). V případě, že faktura nebude mít odpovídající náležitosti, je Objednatel oprávněn zaslat ji ve lhůtě splatnosti zpět Poskytovateli k doplnění či úpravě, aniž se tak dostane do prodlení se splatností; lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného dokladu.
- 5.4 Fakturace bude probíhat vždy na období 1 roku. První faktura bude vystavena následující pracovní den od zahájení plnění na základě potvrzení o zahájení poskytování služby vystaveného Poskytovatelem a potvrzeného kontaktní osobou Objednatele, s datem zdanitelného plnění odpovídajícímu datu zahájení plnění dle čl. 3.1 Smlouvy. Každá další

faktura bude vystavena následující pracovní den po uplynutí předchozího ročního období na základě potvrzení o pokračování poskytování služby vystaveného Poskytovatelem a potvrzeného kontaktní osobou Objednatele, s datem zdanitelného plnění ke dni 22.12. daného kalendářního roku.

- 5.5 Doba splatnosti daňového dokladu, faktury vystavené Poskytovatelem, bude 30 kalendářních dnů ode dne doručení daňového dokladu Objednateli.
- 5.6 Povinnost zaplatit fakturu je splněna dnem odepsání fakturované částky z účtu Objednatele ve prospěch účtu Poskytovatele.
- 5.7 Fakturace probíhá výhradně elektronicky. Objednateli bude faktura zaslána elektronicky na e-mailovou adresu [opava@suip.cz](mailto:opava@suip.cz) a e-mailovou adresu kontaktní osoby Objednatele.
- 5.8 Objednatel nebude poskytovat jakékoli zálohové platby.
- 5.9 Poskytovatel výslovně uvádí, že před uzavřením této Smlouvy správce daně vůči němu nerozhodl, že je ve smyslu § 106a ZoDPH tzv. nespolehlivým plátcem. Pakliže bude správcem daně následně rozhodnuto, že Poskytovatel nespolehlivým plátcem je, je Poskytovatel povinen o tom informovat Objednatele, a to do 5 pracovních dnů od doručení rozhodnutí Poskytovateli; Poskytovatel je srozuměn s tím, že v takovém případě mu bude daň z přidané hodnoty uhrazena až poté, co Objednateli doloží, že příslušnému správci daně daň z přidané hodnoty uhradil.

## 6. Kontaktní osoby

### 6.1 Zástupce Objednatele

Jméno a příjmení: [REDACTED]  
Funkce: vedoucí úseku IT  
Telefon: [REDACTED]  
Email: [REDACTED]

### 6.2 Odpovědná osoba oprávněná jednat ve věcech ZKB

Jméno a příjmení: [REDACTED]  
Funkce: pověřenec pro ochranu osobních údajů a manažer kybernetické bezpečnosti  
Telefon: [REDACTED]  
Email: [REDACTED]

Objednatel podpisem Smlouvy potvrzuje, že výše uvedené kontaktní osoby jsou oprávněny zastupovat Objednatele ve věcech jim určených Smlouvou, s výjimkou činění úkonů, kterými by docházelo ke změně Smlouvy. Kontaktní osoba Objednatele dle čl. 6.1 Smlouvy (tj. v čl. 6.1 Smlouvy uvedený zástupce Objednatele) je oprávněna určit (dalšího) zástupce Objednatele ve smyslu čl. 7 Smlouvy.

### 6.3 Zástupce Poskytovatele

Jméno a příjmení: [REDACTED]  
Funkce: Channel Development Manager  
Telefon: [REDACTED]  
Email: [REDACTED]

### 6.4 Odpovědná osoba oprávněná jednat ve věcech ZKB

Jméno a příjmení: [REDACTED]

Funkce: Senior Technical Consultant & Project Coordinator  
Telefon: [REDACTED]  
Email: [REDACTED]

Poskytovatel podpisem Smlouvy potvrzuje, že výše uvedené kontaktní osoby jsou oprávněny zastupovat Poskytovatele ve věcech jim určených Smlouvou, s výjimkou činění úkonů, kterými by docházelo ke změně Smlouvy.

- 6.5 Případnou změnu kontaktních osob jsou smluvní strany povinny neprodleně prokazatelně oznámit druhé smluvní straně. V tomto případě se ustanovení čl. 13.11 Smlouvy nepoužije.

## 7. Odpovědnost za vady, záruka, odpovědnost za škodu, servisní podmínky

- 7.1 Poskytovatel je povinen poskytovat služby sjednané Smlouvou řádně a včas.
- 7.2 Poskytovatel je povinen realizovat veškeré služby sjednané Smlouvou na svůj náklad a na své nebezpečí.
- 7.3 Poskytovatel se zavazuje poskytovat služby ve standardní kvalitě, v dohodnutém rozsahu, bez jakýchkoli právních či faktických vad a v dohodnutých lhůtách. Případné vady plnění nebo konkrétního druhu zboží je Objednatel povinen reklamovat bez zbytečného prodlení po jejich zjištění.
- 7.4 Odpovědnost Poskytovatele za škodu či jinou újmu a nároky z ní vyplývající se řídí ustanoveními § 2913 a násl. občanského zákoníku. Hradí se skutečná škoda či jiná újma a ušlý zisk. Výše škody či jiné újmy není stranami omezena. Škoda se hradí v penězích nebo, je-li to možné nebo účelné, uvedením do předešlého stavu podle volby Objednatele v konkrétním případě.
- 7.5 Poskytovatel se zavazuje zajišťovat dosahování takové kvality služeb a za takových podmínek, jak je definováno v této Smlouvě. Poskytovatel je srozuměn s tím, že poskytované servisní služby, tj. služby dle této Smlouvy, budou předmětem tzv. SLA hodnocení, včetně sankčních ujednání k SLA.
- 7.6 V rámci poskytování servisních služeb, tj. služeb dle této Smlouvy, je Poskytovatel povinen řešit incidenty týkající se předmětu plnění (dále jen „**incidenty**“) a požadavky Objednatele (dále jen „**požadavky**“) za podmínek sjednaných touto Smlouvou.
- 7.7 Poskytovatel je povinen při poskytování servisních služeb, tj. služeb dle této Smlouvy, reagovat na zástupcem Objednatele nahlášený incident nebo požadavek potvrzením přijetí hlášení incidentu nebo požadavku a odpovědí zástupci Objednatele s informací o předpokládané době potřebné na vyřešení v případě požadavku. Doba mezi nahlášením incidentu nebo požadavku a odpovědí Poskytovatele Objednateli se pro účely této Smlouvy dále nazývá „**reakční doba**“.
- 7.8 Poskytovatel je povinen vyřešit Objednatelem nahlášený incident nebo požadavek dle tabulky definice kvality služeb (SLA) uvedené v čl. 7.9 a 7.10 Smlouvy. Doba mezi nahlášením incidentu nebo požadavku a vyřešením incidentu nebo požadavku se pro účely této Smlouvy dále nazývá „**doba vyřešení**“.
- 7.9 **Incidenty**
- 7.9.1 dostupnost online servisní podpory garantuje Poskytovatel v pracovních dnech v době od 8 do 16 hodin, řešení problému formou vzdáleného přístupu VPN garantuje Poskytovatel v termínech a časech dohodnutých s Objednatelem.

### 7.9.2 Definice kvality služeb (SLA):

Kategorie incidentu	Reakční doba	Doba vyřešení
Nízká - na provoz systému DLP má pouze zanedbatelný vliv.	1 pracovní den	Max do 3 pracovních dnů, nebude-li dohodnuto se zástupcem Objednatele jinak

7.9.3 Incidentem se rozumí výpadek poskytování podpory garantované dle technické specifikace, tj. dle přílohy č. 2 Smlouvy, která neprobíhá očekávaným způsobem a její nedostupnost omezuje či může omezit funkce systému DLP nebo způsobí či může způsobit nedostupnost systému DLP (např. výpadek, výrazné zpomalení systému DLP na základě SW poruchy nebo SW chyby na informačních systémech, vzniklá nedostupnost dat, nedostupnost komunikací atp.). Incidentem je i jakýkoliv zjištěný bezpečnostní problém, a to i v případě, že neohrožuje okamžitě dostupnost a funkce systému.

7.9.4 Poskytovatel se zavazuje reagovat na Objednatelem nahlášený incident dle tabulky definice kvality služeb (SLA).

### 7.9.5 Sankční ujednání k ujednání o kvalitě služeb (SLA)

Kategorie incidentu	Sankce za porušení <b>reakční doby</b> , a to za každý započatý pracovní den prodlení	Sankce za porušení <b>doby vyřešení</b> , a to za každý započatý den prodlení
Nízká	1 000,- Kč	1 000,- Kč

## 7.10 **Požadavky**

7.10.1 Poskytovatel bude plnit požadavky Objednatele následovně:

### 7.10.2 Definice kvality služeb (SLA):

Požadavky	Reakční doba	Doba vyřešení
Požadavky na řešení problémů formou vzdáleného VPN přístupu pracovníka poskytovatele na server SÚIP (Objednatele)	nejpozději do následujícího pracovního dne, nebude-li dohodnuto se zástupcem Objednatele jinak	nejpozději do 3 pracovních dnů, nebude-li dohodnuto se zástupcem Objednatele jinak
Ostatní požadavky	nejpozději do následujícího pracovního dne, nebude-li dohodnuto se zástupcem Objednatele jinak	nejpozději do 3 pracovních dnů, nebude-li dohodnuto se zástupcem Objednatele jinak

### 7.10.3 Sankční ujednání k ujednání o kvalitě služeb (SLA)

Kategorie požadavku	Sankce za porušení <b>reakční doby</b> , a to za každý i jen započatý pracovní den prodlení	Sankce za porušení <b>doby vyřešení</b> , a to za každý i jen započatý pracovní den prodlení
	1 000,- Kč	1 000,- Kč

## **8. Sankční podmínky**

- 8.1 V případě, že Poskytovatel nezahájí plnění řádným způsobem a v dohodnutém čase plnění dle čl. 3.1 Smlouvy, zaplatí Objednateli smluvní pokutu ve výši 0,25 % z celkové ceny plnění (tj. Ceny vč. DPH dle čl. 5.1 Smlouvy) za každý den prodlení.
- 8.2 Poruší-li Poskytovatel některou z povinností podle čl. 10.4, 10.6, 10.8, 10.11 až 10.15, 10.26 a 10.27 Smlouvy, je povinen uhradit Objednateli smluvní pokutu ve výši 40 000,- Kč za každé jednotlivé porušení; poruší-li Poskytovatele jakoukoliv jinou z povinností vyjmenovaných v čl. 10. Smlouvy je povinen uhradit Objednateli 20 000,- Kč za každé jednotlivé porušení.
- 8.3 V případě zjištění nepravdivosti prohlášení „ano“ Poskytovatele v ČÁSTI I. – Standardy Dotazníku pro hodnocení úrovně kybernetické bezpečnosti účastníka, který tvoří Přílohu č. 3 Smlouvy (dále také jen „Dotazník“) nebo zjištění, že není vydán certifikát dokládající stejnou úroveň kvality na další období dle čl. 10.4 Smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši dle čl. 8.2 věty první před středníkem (tj. ve výši 40 000,- Kč za každé jednotlivé porušení).
- 8.4 Poskytovatel je povinen zaplatit smluvní pokutu Objednateli, pokud způsob poskytování servisních služeb, tj. služeb dle této Smlouvy, je v rozporu s požadavky na servisní služby vymezenými čl. 7.9 a 7.10 Smlouvy (SLA). Smluvní pokutu hradí Poskytovatel Objednateli ve výši a případech stanovených v čl. 7.9 a 7.10 Smlouvy, v těchto případech tak Poskytovatel nehradí smluvní pokutu dle čl. 8.1 ani žádnou ze smluvních pokut dle jiných článků Smlouvy.
- 8.5 V případě porušení jakékoliv povinnosti stanovené ve Smlouvě se Poskytovatel zavazuje zaplatit Objednateli smluvní pokutu ve výši 0,5 % z celkové ceny plnění (tj. Ceny vč. DPH dle čl. 5.1 Smlouvy) za každý jednotlivý případ porušení povinnosti Poskytovatele. To se netýká případů dle čl. 8.1 až 8.4 Smlouvy.
- 8.6 Pokud bude Objednatel v prodlení s úhradou faktury proti sjednanému termínu, je povinen zaplatit Poskytovateli zákonný úrok z prodlení.
- 8.7 Poskytovatel se zavazuje zaplatit Objednateli smluvní pokutu nejpozději do 30 dnů ode dne, kdy bude Objednatelem o vzniklém porušení a výši následné sankce prokazatelně informován.
- 8.8 Uplatnění sankcí ze strany Objednatele nezbavuje Poskytovatele povinnosti dodatečně splnit stanovenou povinnost.
- 8.9 Zaplacením smluvní pokuty není dotčeno právo Objednatele na náhradu škody vzniklé v příčinné souvislosti s prodlením či porušením povinnosti Poskytovatele.
- 8.10 Objednatel si vyhrazuje právo na úhradu smluvní pokuty formou zápočtu ke kterékoliv splatné pohledávce Poskytovatele vůči Objednateli.
- 8.11 V případě uplatnění smluvní pokuty nezaniká nárok na náhradu případné škody.

## **9. Ochrana osobních údajů**

- 9.1 Smluvní strany jsou správci osobních údajů vykonávajících samostatnou činnost, která nezakládá povinnost uzavřít zpracovatelskou smlouvu dle čl. 28 GDPR, když předmětem plnění ze strany Poskytovatele není systematické zpracování osobních údajů subjektů osobních údajů spravovaných Objednatelem a ke zpřístupnění osobních údajů Poskytovateli může dojít pouze náhodně, v omezené míře, v souvislosti s řešením konkrétního problému formou vzdáleného VPN přístupu na server SÚIP (Objednatele). Smluvní strany se zavazují zajistit při plnění

Smlouvy ochranu osobních údajů svých zaměstnanců, příp. i dalších osob. Smluvní strany se zavazují postupovat v souvislosti s plněním Smlouvy v souladu s platnými a účinnými právními předpisy na ochranu osobních údajů, zejména dle zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů a dle nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů, GDPR). Pokud bude smluvní strana v souvislosti s plněním Smlouvy zpracovávat osobní údaje zaměstnanců/kontaktních osob druhé smluvní strany (jméno, telefon, e-mail, popř. další), zavazuje se zpracovávat tyto osobní údaje pouze v rozsahu nezbytném pro plnění Smlouvy, a po dobu nezbytně nutnou. Informace o zpracování osobních údajů ze strany Státního úřadu inspekce práce (Objednatele) u dotčených fyzických osob jsou uvedeny na internetových stránkách <https://www.suip.cz/web/suip/gdpr>.

## **10. Zajištění mlčenlivosti, bezpečnosti informací a požadavků zákona o kybernetické bezpečnosti**

- 10.1 Tato Smlouva je uzavírána v souladu s aktuálními právními předpisy upravujícími kybernetickou bezpečnost. Tato Smlouva bude Poskytovatelem plněna v souladu s aktuálními právními předpisy, zejména v souladu s ustanoveními ZKB a VKB; pokud dojde k významné legislativní změně v oblasti kybernetické bezpečnosti významných informačních systémů, bude uzavřen dodatek k této smlouvě.
- 10.2 Smluvní strany uvádí, že je jim známo, že Objednatel je správcem významných informačních systémů ve smyslu § 2 odst. 1 písm. a) a b) vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů, a dle § 3 písm. e) ZKB. Objednatel považuje Poskytovatele za významného dodavatele ve smyslu ust. § 2 písm. n) VKB. Poskytovatel je povinen při plnění Smlouvy zajistit dodržování požadavků na kybernetickou bezpečnost a prohlašuje, že při své činnosti postupuje v souladu se ZKB a VKB a dále v souladu s technickými standardy ISO 27001 o zajištění bezpečnosti informací nebo jiným rovnocenným řešením. Poskytovatel bere na vědomí, že je Objednatel veden v jeho evidenci významných dodavatelů.
- 10.3 Využívá-li Poskytovatel při plnění Smlouvy poddodavatele, je Poskytovatel povinen zajistit, aby jeho poddodavatelé byli smluvně zavázáni vůči němu ve stejném rozsahu, jako je zavázán Poskytovatel vůči Objednateli, tj. poddodavatel je povinen vůči Poskytovateli dodržovat stejná smluvní ujednání, která je povinen dodržovat Poskytovatel vůči Objednateli dle této Smlouvy. To platí rovněž na další články poddodavatelského řetězce.
- 10.4 Poskytovatel se zavazuje, že zavede bezpečnostní opatření v souladu s bezpečnostními požadavky Objednatele uvedenými v této Smlouvě a jejich přílohách, popř. s bezpečnostními požadavky relevantních třetích stran, pro formu přístupu uvedeného v čl. 10.6 Smlouvy a bude je monitorovat a vyhodnocovat jejich účinnost. Poskytovatel prohlašuje, že má zavedena všechna bezpečnostní opatření, procesy a technologie, které prohlásil za zavedené (odpověděl ANO) v Dotazníku. Poskytovatel se dále zavazuje, že pokud by v době trvání Smlouvy mělo dojít ke skončení platnosti některého z certifikátů kvality doloženého k prohlášení v ČÁSTI I. – STANDARDY Dotazníku při podání nabídky, zajistí vydání certifikátu dokládajícího stejnou úroveň kvality na další období tak, aby tato úroveň kvality trvala po celé smluvní období.
- 10.5 Informace a data poskytnutá ze strany Objednatele Poskytovateli jsou majetkem Objednatele.
- 10.6 Poskytovateli může být při řešení konkrétního problému v rámci vzdáleného, časově omezeného a logovaného přístupu VPN umožněn přístup k důvěrným informacím Objednatele, např. k osobním údajům zaměstnanců Objednatele a dalších osob, které jsou pro účely zajištění bezpečnosti informací v souladu s Přílohou 1 VKB z hlediska důvěrnosti, integrity a dostupnosti Objednatel hodnoceny takto:



- 10.6.1 důvěrnost – prevence neautorizovaného vyzrazení dat: úroveň 3, vysoká;
- 10.6.2 integrita – prevence neautorizované úpravy dat: úroveň 3, vysoká;
- 10.6.3 dostupnost – prevence ztráty přístupu k datům: úroveň 3, vysoká.

Poskytovatel se zavazuje z hlediska zajištění důvěrnosti, integrity a dostupnosti důvěrných informací Objednatele pro výše uvedenou formu vzdáleného přístupu minimalizovat rizika na své straně, a to jak technická, tak personální.

- 10.7 Poskytovatel je povinen přijmout vhodná technická a organizační opatření přiměřená okolnostem zpracování, která zabrání ztrátě, zničení či pozměnění informací a dat a neoprávněnému či nahodilému přístupu k nim nebo jejich neoprávněnému či nahodilému zpřístupnění na straně Poskytovatele.
- 10.8 Poskytovatel je povinen zachovávat mlčenlivost o všech skutečnostech, informacích a osobních údajích (zejména, avšak nikoli výlučně, finanční, technické, organizační nebo ekonomické povahy), které jsou obsaženy ve Smlouvě a dále o všech skutečnostech a informacích, které mu byly v souvislosti se Smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl v souvislosti se Smlouvou, vyjma těch, které jsou v okamžiku, kdy se s nimi Poskytovatel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění Poskytovatele veřejně přístupnými stanou (dále jen „důvěrné informace“). Poskytovatel nesmí takové skutečnosti a informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Objednatele.
- 10.9 Jakékoliv operace ze strany Poskytovatele vůči nepovolaným osobám s informacemi či daty poskytnutými Objednatelem musí být dopředu prokazatelně odsouhlaseny Objednatelem.
- 10.10 Povinnost mlčenlivosti ve vztahu k důvěrným informacím se nevztahuje na případy, kdy:
  - 10.10.1 předmětná důvěrná informace je obecně známa a v obecnou známost vešla bez zavinění příslušné smluvní strany;
  - 10.10.2 existuje zákonná povinnost sdělit příslušnou důvěrnou informaci;
  - 10.10.3 předmětná důvěrná informace je uplatněna v rámci soudního řízení (včetně řízení o výkon rozhodnutí či řízení o nařízení exekuce) mezi smluvními stranami (včetně jejich právních nástupců), případně mezi smluvní stranou a třetí osobou, jedná-li se o spor vyplývající z této Smlouvy a v případě dalších vztahů s touto Smlouvou souvisejícími;
  - 10.10.4 důvěrná informace je sdělována osobě, která je vázána stejnou či přísnější povinností mlčenlivosti, zejména je-li sdělována advokátovi;
  - 10.10.5 je důvěrná informace sdělována subjektu, na nějž přechází zákonné kompetence Objednatele, v souvislosti, s nimiž je plnění užíváno.
- 10.11 Poskytovatel je povinen své poddodavatele zavázat k mlčenlivosti v rozsahu daném touto Smlouvou, po čemž je oprávněn poskytovat v nezbytně nutném rozsahu informace svým poddodavatelům.
- 10.12 Obě smluvní strany jsou povinny k ochraně důvěrných informací zavázat všechny osoby a subjekty, které mají k plnění předmětu této Smlouvy přístup nebo kterým poskytly či sdělily důvěrné informace dle ustanovení uvedených v tomto článku.
- 10.13 Součástí povinnosti mlčenlivosti je povinnost smluvních stran učinit vše, co je v jejich silách, aby důvěrné informace nevyšly ve známost nepovolaným osobám.

- 10.14 Povinnost zachovávat mlčenlivost trvá i po skončení účinnosti této Smlouvy, vyjma případů, kdy se takové skutečnosti a informace stanou prokazatelně veřejně přístupné bez zavinění Poskytovatele.
- 10.15 Poskytovatel se zavazuje provádět služby v termínech a časech dle čl. 7.9 Smlouvy tak, aby nedošlo k výpadku systému DLP Objednatele. Výpadek nesmí přesáhnout dobu vyřešení stanovenou v čl. 7.9 a 7.10 Smlouvy.
- 10.16 Poskytovatel bude v rámci provádění a poskytování služby používat výhradně zabezpečený a monitorovaný přístup do ICT systému Objednatele.
- 10.17 Poskytovatel se zavazuje, že vzdálený přístup do systému bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.
- 10.18 Poskytovatel se zavazuje zajistit, aby osoby Poskytovatele podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo systému ICT Objednatele, užívali notebook nebo počítač nebo tablet s aplikovanými bezpečnostními záplatami a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranou.
- 10.19 Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokovan a řešen jako bezpečnostní incident. Poskytovatel bere na vědomí, že postup zvládnutí bezpečnostního incidentu či jiný důsledek porušení bezpečnostních požadavků nebude posuzován jako okolnost vylučující odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoliv náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele.
- 10.20 Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části systému ICT programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci systému ICT nebo nelegální získání dat a informací.
- 10.21 Poskytovatel bere na vědomí, že veškerá jeho aktivita a jeho plnění realizované v systémovém prostředí Objednatele budou Objednatelům průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy.
- 10.22 Poskytovatel i Objednatel se vzájemně zavazují informovat se o všech přijatých bezpečnostních opatřeních ve smyslu příslušných ustanovení ZKB a poskytovat si navzájem součinnost při řízení kontinuity činností.
- 10.23 Objednatel má oprávnění zapojit Poskytovatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Poskytovatele do plánu kontinuity činností, který souvisí s předmětem této Smlouvy a souvisejících služeb.
- 10.24 Poskytovatel je povinen informovat Objednatele o způsobu řízení rizik přijatém Poskytovatelem a o zbytkových rizicích na straně Poskytovatele souvisejících s plněním této Smlouvy, jakož i o způsobu, jak tato rizika budou řešena, přičemž zvoleným způsobem bude co nejvíce minimalizováno riziko narušení bezpečnosti informací a dat Poskytovatele.
- 10.25 Poskytovatel je povinen na výzvu provést export dat nebo jejich části ze systému a předat data Objednateli, a to jak v průběhu trvání této Smlouvy, tak při jejím ukončení.
- 10.26 V případě kybernetických bezpečnostních událostí a incidentů na straně Poskytovatele, které souvisí nebo by mohly souviset s předmětem plnění této Smlouvy a mají potenciální negativní dopad na Objednatele, je Poskytovatel povinen bez zbytečného odkladu informovat Objednatele datovou zprávou, e-mailem na e-mail: [incidentyKB@suip.cz](mailto:incidentyKB@suip.cz) a též telefonicky odpovědné osobě oprávněné jednat ve věcech ZKB dle čl. 6.4 Smlouvy. Poskytovatel je povinen bez zbytečného odkladu přijmout opatření nezbytná k zamezení či minimalizaci škod a zároveň přijmout bezpečnostní opatření zamezující opakování kybernetických bezpečnostních událostí a incidentů.

- 10.27 Poskytovatel je povinen obratem informovat Objednatele stejnými informačními kanály uvedenými v předchozím odstavci Smlouvy, nejpozději následující pracovní den, o způsobu vyřešení bezpečnostních událostí a incidentů a o bezpečnostních opatřeních, která přijal dle čl. 10.26 Smlouvy.
- 10.28 Objednatel má právo u Poskytovatele provést (a to i opakovaně) zákaznický audit v oblasti kybernetické bezpečnosti pro účely plnění požadavků ZKB a požadavků VKB a kontrolu požadavků vyplývajících z této Smlouvy. Zákaznický audit/kontrola je Objednatelem prováděn na základě předchozí výzvy Objednatele. Tato výzva Objednatele bude obsahovat termín zákaznického auditu/kontroly a bude doručena Poskytovateli nejpozději 10 dní před plánovaným termínem provedení zákaznického auditu/kontroly; termín zákaznického auditu/kontroly lze po domluvě se Poskytovatelem změnit. Při provádění zákaznického auditu/kontroly bude vždy přihlédnuto k povaze a rozsahu plnění dle této Smlouvy. Rozsah zákaznického auditu/kontroly bude specifikován ve výzvě Objednatele. Zákaznický audit/kontrola může být vykonán přímo zaměstnanci Objednatele, případně prostřednictvím třetí osoby Objednatelem pověřené. Zákaznický audit/kontrola může být proveden max. 1x za kalendářní rok. Poskytovatel poskytne Objednateli při provádění zákaznického auditu/kontroly nezbytnou součinnost. Objednatel zákaznický audit/kontrolu provádí jen v nezbytném rozsahu a prostřednictvím nejmenšího nezbytného počtu osob.
- 10.29 Poskytovatel má povinnost bez zbytečného odkladu informovat Objednatele o významné změně ovládání Poskytovatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, nebo změně vlastnictví zásadních aktiv, jakož i změně v oprávnění Poskytovatele nakládat s těmito aktivy, které jsou využívány k plnění předmětu Smlouvy.
- 10.30 V případě, že u Poskytovatele dojde k významné změně ovládání či řízení Poskytovatele dle § 71 a následujících zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, má Objednatel právo odstoupit od Smlouvy.

## **11. Ostatní ujednání**

- 11.1 Tvoří-li Poskytovatele více osob, platí následující:
- 11.1.1 všechny osoby tvořící Poskytovatele jsou ze Smlouvy zavázány společně a nerozdílně,
  - 11.1.2 jednání kterékoli z osob tvořících Poskytovatele je přičítáno Poskytovateli bez ohledu na vnitřní vztahy mezi jednotlivými osobami tvořícími Poskytovatele,
  - 11.1.3 za Poskytovatele může jednat kterákoli z osob tvořících Poskytovatele, tím není dotčen zejména čl. 6 Smlouvy.
- 11.2 Poskytovatel je povinen neprodleně písemně informovat Objednatele o skutečnostech majících i potencionálně vliv na plnění jeho povinností vyplývajících ze Smlouvy, a není-li to možné, nejpozději následující den poté, kdy příslušná skutečnost nastane nebo Poskytovatel zjistí, že by nastat mohla. Současně je Poskytovatel povinen učinit veškeré nezbytné kroky vedoucí k eliminaci případné škody hrozící Objednateli, a to zejména obstarat neprodleně náhradní plnění (tím není dotčen zejména čl. 6 a 10.3 Smlouvy), přičemž je povinen nést případný rozdíl ceny.
- 11.3 Poskytovatel není oprávněn provést jednostranné započtení žádné své pohledávky za Objednatelem vyplývající ze Smlouvy nebo vzniklé v souvislosti se Smlouvou na jakoukoliv pohledávku Objednatele za Poskytovatelem.
- 11.4 Poruší-li Poskytovatel v souvislosti se Smlouvou jakoukoli svoji povinnost, nahradí Objednateli škodu a nemajetkovou újmu z toho vzniklou. Povinnosti k náhradě se Poskytovatel zproutí,

prokáže-li, že mu ve splnění povinnosti zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá z osobních poměrů Poskytovatel nebo vzniklá až v době, kdy byl Poskytovatel s plněním povinnosti v prodlení, ani překážka, kterou byl Poskytovatel povinen překonat, jej však povinnosti k náhradě nezproští.

- 11.5 Písemnou formou (podobou) se rozumí listina podepsaná oprávněnou osobou smluvní strany nebo e-mail podepsaný zaručeným elektronickým podpisem oprávněné osoby smluvní strany.

## **12. Pojištění**

- 12.1 Poskytovatel se zavazuje, že bude mít od zahájení plnění dle čl. 3.1 smlouvy vyplývajícího ze Smlouvy sjednáno pojištění odpovědnosti za škodu či jinou újmu způsobenou Poskytovatelem při výkonu činnosti třetí osobě s limitem pojistného plnění minimálně ve výši Ceny vč. DPH, přičemž spoluúčast nebude vyšší než 5 (pět) % z limitu pojistného plnění. V případě, že Smlouvu uzavřelo na straně Poskytovatele více osob (členů sdružení, členů společnosti apod.), musí pojistná Smlouva prokazatelně pokrývat případnou škodu způsobenou kteroukoli z těchto osob.
- 12.2 Poskytovatel je povinen předložit Objednateli pojistnou Smlouvu nebo pojistku osvědčující splnění povinnosti Poskytovatele podle čl. 12.1 Smlouvy kdykoli v průběhu trvání závazků ze Smlouvy, a to do 5 pracovních dní od vyzvání ze strany Objednatele.
- 12.3 Poskytovatel i Objednatel se zavazují uplatnit pojistnou událost u pojišťovny bez zbytečného odkladu.

## **13. Závěrečná ustanovení**

- 13.1 Má-li smluvní strana datovou schránku, považují se veškeré zaslané zásilky za doručené dnem dodání do datové schránky druhé smluvní strany, a to včetně odstoupení od Smlouvy.
- 13.2 Není-li stanoveno jinak, řídí se tento smluvní vztah příslušnými ustanoveními občanského zákoníku.
- 13.3 Smluvní strany na sebe přebírají nebezpečí změny okolností dle § 1765 odst. 2 občanského zákoníku.
- 13.4 Pokud by jednotlivá ustanovení Smlouvy byla zcela či částečně neplatná nebo neproveditelná, nebude tím dotčena platnost či proveditelnost zbývajících ustanovení. Namísto neplatného ustanovení bude platit za dohodnuté takové platné ustanovení, které nejbližší odpovídá smyslu a účelu neplatného ustanovení. Pokud by se v důsledku změny právních předpisů nebo z jiných důvodů stala některá ujednání Smlouvy v budoucnosti neplatnými nebo neúčinnými, budou tato ustanovení uvedena do souladu s právními normami a smluvní strany prohlašují, že Smlouva je ve zbývajících ustanoveních platná, neodporuje-li to jejímu účelu nebo nejedná-li se o ustanovení, která oddělit nelze.
- 13.5 Poskytovatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou plnění nebo služeb z veřejných výdajů.
- 13.6 Poskytovatel bere na vědomí, že Objednatel je povinný subjekt k poskytování informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.
- 13.7 Smluvní strany sjednávají, že žádné z údajů obsažené ve Smlouvě a jejích přílohách nejsou považovány za obchodní tajemství dle § 504 občanského zákoníku. V případě, že by Poskytovatel trval na tom, že některý údaj obsažený ve Smlouvě a jejích přílohách je

obchodním tajemstvím a následně vyšlo najevo, že údaj nenaplňoval podmínky stanovené v § 504 občanského zákoníku, za nesprávné označení údaje za obchodní tajemství nese odpovědnost Poskytovatel.

- 13.8 Objednatel a Poskytovatel vynaloží veškeré úsilí, aby všechny spory, které vyplynou ze Smlouvy nebo v souvislosti s ní, byly urovnány především oboustrannou dohodou. Sdělení o existujících neshodách, případně rozporech se Smlouvou bude zasláno písemně doporučeným dopisem druhé straně (popř. pokud má Poskytovatel k dispozici datovou schránkou jejím prostřednictvím).
- 13.9 Jestliže nebude možné přes veškerou snahu spor vyřešit dohodou, bude řešen soudní cestou, a to místně a věcně příslušnými soudy. Rozhodným právem pro řešení sporů je právo české.
- 13.10 Poskytovatel není oprávněn postoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy nebo vzniklou v souvislosti se Smlouvou. Totéž platí o postoupení Smlouvy.
- 13.11 Smlouva může být měněna nebo doplňována pouze písemnými dodatky odsouhlasenými oběma stranami.
- 13.12 Smlouva je sepsána v českém jazyce.
- 13.13 Smlouva je sepsána v českém jazyce ve dvou stejnopisech, z nichž po jednom obdrží každá ze smluvních stran
- 13.14 Smluvní strany prohlašují, že Smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz souhlasu s jejím obsahem připojují svoje podpisy.

#### **Přílohy:**

Příloha č. 1 Rozsah plnění dle smlouvy o dílo uzavřené dne 21. 10. 2021

Příloha č. 2 Technická specifikace a kalkulace nabídkové ceny plnění

Příloha č. 3 Dotazník pro hodnocení úrovně kybernetické bezpečnosti

#### **Poskytovatel:**

Safetica a.s.

Místo, datum V Brně dne  
Jméno Ing. Richard Brulík  
Pozice Člen představenstva

Podpis

.....

#### **Objednatel:**

ČR – Státní úřad inspekce práce

Místo, datum V Opavě dne  
Jméno Mgr. Ing. Rudolf Hahn  
Pozice Generální inspektor SUIP

Podpis

.....

## Technická specifikace - minimální požadavky

Minimální požadavky zadavatele	Údaje vyplněné účastníkem	
	Splnění požadavků ANO/NE	Bližší popis, hodnota
Centrální administrátorská konzole	ANO	
Autonomní řízení přístupu do nastavení konzole	ANO	
Autonomní řízení přístupu k administraci SW	ANO	
Autonomní řízení přístupu k logům	ANO	
Tichý režim běhu na stanicích uživatelů (users)	ANO	
Tichý režim běhu na stanicích uživatelů s vyššími právy (min. lokální a doménoví administrátoři)	ANO	
Ochrana proti změně nastavení, zastavení a odinstalaci SW uživatelem i uživatelem s vyššími právy	ANO	
Automatický restart nebo jiná forma obnovy činnosti SW v případě zastavení uživatelem s vyššími právy	ANO	Uživatel není schopen (ani s administrátorskými právy) zastavit Safetica klienta na své stanici. Jediný způsob, jak může uživatel Safetica klienta zastavit je, pokud mu Safetica administrátor toto právo přes Safetica konzoli udělí a pokud uživatel zná heslo na lokální administraci (taktéž definované v Safetica administrátorské konzoli).
Ochrana proti editaci registrů, systémových komponent či knihoven SW	ANO	Safetica chrání svoje systémové procesy a registrové klíče a také všechny knihovny a schované instalační složky.
Veškeré funkce SW musí být zachovány i v offline módu	ANO	
Ochrana proti přihlášení uživatele do safe módu	ANO	
Funkce zálohování komponent systému, zejména nastavení a záznamů	ANO	Safetica umožňuje nastavení pravidelných zálohovacích úloh databáze. Vytvořené archivy se následně dají opětovně připojit ke konzoli pro náhled starších dat. Kromě databáze lze zálohovat rovněž i nastavení a záznamy.
Automatická emailová notifikace incidentů s možností změny nastavení	ANO	Safetica umožňuje nastavení emailových notifikací v případě incidentů či porušení bezpečnostních politik. Tyto notifikace jsou odeslány okamžitě po incidentu. Nastavení emailových notifikací lze v produktu operativně měnit.
Automatický emailový reporting s možností změny nastavení	ANO	Safetica umožňuje nastavení předdefinovaných automatických reportů, nebo reportů s přizpůsobeným vlastním obsahem. Nastavení emailových reportů lze v produktu operativně měnit.
Práce s historickými daty min. 90 dnů zpět	ANO	Jediný limit práce s daty je velikost databáze a je jen na Vás, kolik živých dat v databázi budete uchovávat. V případě poskytnutí adekvátního diskového prostoru pro databázi ze strany zadavatele, umožní aplikace práci s historickými daty minimálně 90 dnů zpět.
Možnost reportingu do SIEM systémů	ANO	Safetica umožňuje zasílání varování a informací o přístupu a změně nastavení do jakéhokoliv SIEM systému poporučícího syslog.
Funkce monitoringu aplikací (čas spuštění, aktivní využívání apod.)	ANO	Safetica sleduje aktivní čas strávený v aplikaci, časový interval, název aplikace, umístění aplikace, název počítače, uživatele a další. Produkt zobrazuje hodnotu "od-do", tedy časový interval běhu aplikace, od jejího spuštění (čas spuštění) až do jejího ukončení.
Funkce kategorizace aplikací	ANO	Safetica software obsahuje vlastní kategorizační databázi aplikací a webů. Je také možné změnit kategorii záznamů či tvořit vlastní kategorie.
Funkce monitoringu www, jejich aktivní využití, URL, protokol, hlavičky www bez ohledu na použitý prohlížeč	ANO	Safetica sleduje aktivní čas strávený na webové stránce, časový interval, URL, hlavičku, protokol, název počítače, uživatele a další. Podporovány jsou všechny oficiální komerční prohlížeče.
Funkce kategorizace www	ANO	Safetica software obsahuje vlastní kategorizační databázi aplikací a webů. Je také možné změnit kategorii záznamů a tvořit vlastní kategorie.

Monitoring práce se soubory, min. přehled uživatelů a aplikací pracujících se soubory	ANO	Přehled uživatelů, název počítače i aplikace pracující se soubory je zobrazena.
Monitoring operací se soubory (Min. otevření, kopírování, přejmenování, smazání)	ANO	Souborové operace jsou zobrazeny - otevření, kopírování, přejmenování, smazání, přesun, atd.
Monitoring lokalizací a přesunů souborů (min. externí umístění, web, cloud)	ANO	V Safetica je zobrazeno jak původní umístění souboru, tak cílová destinace při přesunu souborů (emailová adresa, webová stránka, cloudová destinace, apod.). Produkt umožňuje kompletní monitoring dat v externích umístěních.
Lokální souborové operace (Min. vytvoření, kopírování, přesun, stahování, FTP, smazání)	ANO	Všechny zmíněné souborové operace jsou v Safetica konzoli zobrazeny.
Otevření souboru včetně zdrojové a cílové destinace (Cesta, typ zařízení)	ANO	Cesta, typ zařízení a další relevantní informace jsou sesbírány. Otevření souboru je monitorováno, a to včetně cesty a typu zařízení na kterém jsou umístěny.
Funkce exportu reportů min. do XLS, PDF	ANO	Report může být vytvořen jako grafický přehled do PDF, nebo jako výpis podrobných informací do XLS.
Logování tiskových úloh	ANO	
Podpora POP3, IMAP, MAPI / Exchange protokolů včetně šifrování	ANO	Ano, včetně šifrování celých emailových zpráv.
Podpora desktopových emailových klientů (Min. MS Outlook), funkce zaznamenávání emailů nezávisle na použité aplikaci	ANO	Desktopové emailové aplikace (klienti), používající MAPI jsou podporované (MS Outlook, Thunderbird, apod.). Emaily jsou zaznamenávány nezávisle na použité aplikaci (min. u MS Outlook).
Podpora záznamu souborů odeslaných přes webové rozhraní email. Klienta	ANO	
Podpora záznamu souborů edeslaných přes IM komunikační nástroje	ANO	
Monitoring základních souborových operací provedených uživatelem na cloudu Office 365 (Min. OneDrive for buss., Sharepoint online)	ANO	Nejen OneDrive for Business a Sharepoint online, ale také OneDrive Personal, Dropbox, Gdrive. Safetica také nabízí rozšířené možnosti integrace s M365 prostředím, díky které uvidíte základní souborové operace na Office 365 cloudu i pokud na ně bylo přistoupeno ze zařízení, které nemají Safetica klienta nainstalovaného.
Záznam emailové komunikace na cloudu Office 365 (Exchange online) všech uživatelů pracujících prostřednictvím aplikace Outlook Web App	ANO	
Možnost monitoringu odeslaných / stažených souborů	ANO	
Logování zapnutí / vypnutí stanice	ANO	
Logování přihlášení / odhlášení uživatele	ANO	
Logování uspání / probuzení stanice	ANO	
Šifrování celých disků včetně systémových	ANO	Safetica nabízí jednoduchou a centrálně řízenou správu MS Bitlocker šifrování pro disky a to jak datových tak systémových.
Šifrování externích USB	ANO	Safetica nabízí jednoduchou a centrálně řízenou správu MS Bitlocker šifrování pro externí zařízení.
Ochrana nezávisle na použitém SW, protokolu, včetně šifrování spojení	ANO	
Ochrana citlivých dat	ANO	
Ochrana dat v případě pokusu o prolomení ochrany, např. pomocí symbolických odkazů na složku	ANO	Ochrana probíhá na hranici koncové stanice, tudíž jsou všechny odchozí soubory chráněny. Ochrana souborů podporuje také metodu symbolických odkazů na složku a je chráněna proti prolomení.
Omezení pohybu jednotlivých kategorií citlivých dat, (Min. vymezení rozsahu zařízení, síť, emailových adres, aplikací a úložišť)	ANO	Restrikce jsou uplatnitelné pomocí DLP datových politik. Výjimky jsou nastavitelné pomocí bezpečných zón (například restrikce posílání citlivých dokumentů přes email, s výjimkou interní firemní domény). Systém umožňuje omezení pohybu vymezením rozsahu zařízení, síť, emailových adres, aplikací a úložišť.
Funkce aplikace politik pro konkrétní aplikace - definice zdroje a cíle (Např. externí zařízení, síť, tisk, virtuální tisk)	ANO	Ano, pomocí aplikačních bezpečnostních politik. Tato funkcionalita je odemčena Enterprise licencí. Lze aplikovat bezpečnostní politiky pro konkrétní aplikace pomocí definicí zdroje.

Funkce aplikace politik pro konkrétní aplikace - správa uživatelských operací (Např. použití schránky, Print screen)	ANO	Nejen kopírování do schránky a printscreenu, ale například i ochrana při sdílení obrazovky.
Správa nepovolených cloudových úložišť	ANO	
Výběr síly preventivních opatření (Min. logování, notifikace, blokace)	ANO	Bezpečnostní politiky mohou fungovat buď v režimu tichého logování (žádné notifikace ani restrikce pro uživatele), notifikací (uživatel má možnost pokračovat s datovým přesunem), či blokace (přesun dat je zakázán).
Funkce definice citlivých dat pomocí předdefinovaných pojmů a algoritmů	ANO	
Definice citlivých dat pomocí vlastních řetězců či regulárních výrazů	ANO	Ano, vše zmíněné.
Funkce importu vlastních slovníků	ANO	
Funkce nastavení počtu výskytu citlivých údajů	ANO	
Dynamické restrikce nad soubory a aplikacemi, pokud je detekován citlivý obsah	ANO	Safetica detekuje citlivý obsah pomocí dynamické služby detekce citlivého obsahu. Systém umožňuje restrikce nad soubory a aplikacemi, pokud je detekován citlivý obsah a tyto restrikce jsou dynamické.
Funkce blokace dat s citlivým obsahem mimo koncovou stanici	ANO	
Správa uživatelských kanálů (Min. email, externí zařízení, web upload, IM nástroje, cloud, síťové disky)	ANO	Všechny popsané kanály jsou podporovány.
Detekce dat s citlivým obsahem na lokálních nebo síťových discích	ANO	
Restrikce pro externí zařízení (Min. USB zařízení, paměťové karty, Bluetooth, optické disky, Fire Wire)	ANO	Ano, vše uvedené.
Funkce integrace s klasifikací třetích stran uložených v metadatech souborů	ANO	Ano.
Monitoring všech připojených zařízení včetně periférií (Min. monitor, myš, klávesnice)	ANO	Pomocí Safetica ovladače externích zařízení. Safetica ovladač externích zařízení je součástí dodávky, tak aby byl prováděn požadovaný monitoring připojených zařízení včetně periférií, a je tedy zhrnut v celkové ceně za Dílo.
Funkce vynucení režimu read only u připojených zařízení	ANO	
CZ lokalizace	ANO	
Oficiální CZ distribuce	ANO	
Podpora OS Windows 10	ANO	
Podpora Windows server 2012, 2016 a 2019	ANO	
Podpora MS SQL 2012 a novějších	ANO	Ano.
Podpora terminálových prostředí	ANO	Ano.
Předinstalační analýza	ANO	
Implementace - Předimplementační analýza rizik ve smyslu rizik nakládání s daty. Monitoring operací s daty vybraných zaměstnanců SÚIP a OIP min. v počtu 80 zaměstnanců (cca 10% všech zaměstnanců) v min. délce trvání 15 pracovních dnů. U každého z těchto uživatelů monitoring min. PC / NTB, tisku, emailu, síťových úložišť, centralizovaných aplikací (zejména VISSS REÚIP), cloudových služeb. Výstupem bude analýza rizik nakládání s daty. Výstupem bude písemný (elektronický formát) vyhodnocení rizik ve smyslu nakládání s daty a statistika jejich používání (report). Možno řešit testovacím nasazením vysoutěženého systému, pokud toto umožňuje. Výstupy z předimplementační analýzy rizik budou použity pro předimplementační bezpečnostní audit.	ANO	Výstupem ze zkušební nasazení softwaru Safetica je Bezpečnostní Audit - report shrnující datovou bezpečnost, využití IT zdrojů a analýza chování uživatelů. Monitoring operací bude realizován v minimálním rozsahu 80 zaměstnanců, minimální délce trvání 15 pracovních dnů a způsobem nasazení systému Safetica na koncové stanice.
Implementace - Integrace s MS Active Directory SÚIP	ANO	
Implementace - Předimplementační penetrační testy v minimálním rozsahu: Phishingový test formou e-mailu, podvržení USB flashdisc nebo jiného média pro přenos dat, test přístupu k síti zadavatele, test přístupu k prostředkům ICT zadavatele, test získání neveřejné informace (např. protokol z kontroly, platový výměr apod.), test fyzických přístupů do lokality (Min. SÚIP + 1X OIP), test vnesení či vynesení předmětu do nebo z lokality. Výstupem bude písemný (elektronický formát) záznam o průběhu jednotlivých penetračních testů (V rozsahu jak, kdy, kde, případně kdo testoval, průběh a výsledek testování), tedy podklad pro předimplementační bezpečnostní audit.	ANO	Předimplementační penetrační testy budou realizovány v rozsahu: Phishingový test formou e-mailu, podvržení USB flashdisc nebo jiného média pro přenos dat, test přístupu k síti zadavatele, test přístupu k prostředkům ICT zadavatele, test získání neveřejné informace (např. protokol z kontroly, platový výměr apod.), test fyzických přístupů do lokality, test vnesení či vynesení předmětu do nebo z lokality. Výstupem bude písemný (elektronický formát) záznam o průběhu jednotlivých penetračních testů (V rozsahu jak, kdy, kde, případně kdo testoval, průběh a výsledek testování), tedy podklad pro předimplementační bezpečnostní audit.



Implementace - Předimplementační bezpečnostní audit ve smyslu vyhodnocení předimplementační analýzy rizik a penetračních testů a návrh implementace SW pro zabezpečení dat.	ANO	
Instalace a Implementace na HW zadavatele	ANO	
Dodání instalační, technické a provozní dokumentace	ANO	
Bezplatná podpora po dobu 1 roku od předání Díla, a to vždy min. telefonicky a e-mailem v době od 8 do 16 hod	ANO	Ano.
<u>Školení administrátorů</u> o počtu max. 12 osob a rozsahu min. 240 minut, max. 480 minut v sídle Objednatele, v min. rozsahu správa, údržba, nastavení a monitoring systému, monitoring výstupů, řešení modelových situací, včetně dodání podkladů pro školení	ANO	Safetica nabízí školení, včetně osobní návštěvy.

## Příloha č. 2 - Technická specifikace a kalkulace nabídkové ceny plnění

## Technická specifikace - minimální požadavky služby

Maintenance DLP software Safetica One Enterprise	Údaje vyplněné účastníkem	
Výrobce / značka / typové označení	Maintenance k SW DLP řešení Safetica One Enterprise + UEBA	
Minimální požadavky zadavatele	Splnění požadavků ANO/NE	Bližší popis, hodnota
Doba trvání plnění služby 4 roky - okamžik zahájení dle čl. 3 Smlouvy	Ano	
Online podpora - v pracovních dnech v době od 8 do 16 hod - telefonicky, emailem nebo prostřednictvím MS Teams. V českém jazyce <i>Uveďte kontaktní místo, údaje pro hlášení poruch</i>	Ano	██
Online znalostní báze v českém jazyce <i>(www nebo ftp)</i>	Ano	██
Možnost stahování nových verzí a aktualizací z webu	Ano	
Řešení problémů formou vzdáleného VPN přístupu pracovníka poskytovatele na server SÚIP	Ano	
Dodání technické a provozní dokumentace aktuální ke dni implementace	Ano	
Dodání aktuální technické a provozní dokumentace v případě nasazení nové verze produktu v době trvání smlouvy do 5-ti pracovních dnů od data vydání této verze	Ano	
Implementace a registrace prodloužení maintenance DLP Software Safetica ONE Enterprise provozované SÚIP	Ano	

## Kalkulace nabídkové ceny

druh plnění	jednotka	jednotková cena bez DPH za 1 rok plnění	nabídková cena celkem bez DPH - za 4 roky	sazba DPH v %	nabídková cena celkem vč. DPH - za 4 roky
Služba - plnění v rozsahu dle čl. 1 Smlouvy	1 rok	383 800,00	1 535 200,00 Kč	21%	1 857 592,00 Kč
<b>Nabídková cena celkem</b>			<b>1 535 200,00 Kč</b>		<b>1 857 592,00 Kč</b>

## Poznámky:

- Jednotkovou cenu uvádějte zaokrouhlenou na 2 desetinná místa.
- Vzorce jsou zaokrouhlovány matematicky na 2 desetinná místa.
- V případě, že účastník není plátcem DPH, vyplní jednotkovou cenu v Kč bez DPH, do pole sazba DPH vyplní 0 a jednotková cena v Kč vč. DPH se bude rovnat jednotkové ceně v Kč bez DPH. Nabídková cena celkem bez DPH, tak bude v případě účastníka výběrového řízení, který není plátcem DPH, rovna nabídkové ceně celkem vč. DPH.

Ing. Richard Brulík

(podpis osoby oprávněné zastupovat jménem či za účastníka, případně razítko)

Příloha č. 6 ZD - Dotazník pro hodnocení úrovně kybernetické bezpečnosti účastníka

Název účastníka (vč. právní formy)	Safetica a.s.
Sídlo/místo podnikání	Laubova 1729/8, 130 00 Praha 3
IČ	25848666

<b>Postup vyplnění:</b>		
A	Účastník odpoví na všechny otázky ano/ne, a to výběrem ve žlutě podbarvených buňkách	
B	Účastník může vymazat hodnotu buňky klávesou Delete.	
C	Bodová hodnota bude vyplněna automatickým výpočtem, stejně jako celkový součet. V části I bude přiděleno za každou odpověď s hodnotou "ano" 15 b, za části II-V bude přiděleno za každou odpověď s hodnotou "ano" 1 b.	
D	Pro účastníka slouží jako kontrolní mechanismus vyplnění všech položek automaticky počítaná hodnota zbývajících nevyplněných hodnot	<b>0</b>

Dotazník	účastník vyplní ano/ne	bodová hodnota
<b>ČÁST I. – Standardy</b>		
1	Které standardy na své informační systémy organizace účastníka aplikuje:	
1.1	ISO 9001 - Systém managementu kvality	ano 15
1.2	ISO/IEC 27001 - Systém managementu bezpečnosti informací	ano 15
<b>ČÁST II. – Základní opatření</b>		
2	Má organizace účastníka manažera kybernetické bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností?	ano 1
3	Byl v organizaci v posledních 12ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti?	ano 1
4	Bylo v organizaci v posledních 12ti měsících provedeno hodnocení rizik v oblasti kybernetické bezpečnosti?	ano 1
5	Které oblasti pokrývá dokument bezpečnostní politiky, pokud v organizaci účastníka existuje?	
5.1	Procesy řízení rizik	ano 1
5.2	Klasifikace aktiv	ano 1
5.3	Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti	ano 1
5.4	Ochrana osobních dat	ano 1
5.5	Identifikace a autentizace uživatelů	ano 1
5.6	Přístup k datům na základě rolí (RBAC, Role Based Access Control)	ano 1
5.7	Řízení privilegovaných přístupů	ano 1
5.8	Ochrana koncových stanic	ano 1
5.9	Ochrana mobilních zařízení a vzdáleného přístupu	ne 0
5.10	Ochrana emailu a vnitrofiremní komunikace (instant messaging)	ano 1
5.11	Ochrana přístupu do internetu	ano 1
5.12	Ochrana médií	ano 1
5.13	Ochrana bezdrátových sítí a komunikace	ano 1
5.14	Bezpečnostní školení koncových uživatelů a administrátorů	ano 1
5.15	Ochrana proti škodlivému softwaru	ano 1
5.16	Ochrana při výměně dat	ano 1
5.17	Procesy zvládnutí kybernetických incidentů	ano 1
5.18	Bezpečnostní audity a analýzy	ano 1
<b>ČÁST III. C – Bezpečnostní technologie</b>		

6	Které níže uvedené bezpečnostní technologie organizace účastníka provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům?		
6.1	Antivirový software na pracovních stanicích	ano	1
6.2	Antivirový software na mobilních zařízeních	ne	0
6.3	Nástroj pro detekci narušení sítě (Intrusion Detection/Prevention System)	ano	1
6.4	Nástroj pro řízení privilegovaných účtů a oprávnění (Privileged Identity Management, Privileged Access Management)	ne	0
6.5	Více-faktorová autentizace	ano	1
6.6	Automatizovaný nástroj pro řízení technologických zranitelností	ne	0
6.7	Nástroj pro řízení přístupu k síti (Network Access Control)	ano	1
6.8	Nástroj pro ochranu před útoky Denial of service a Distributed Denial of Service	ano	1
6.9	Šifrovací nástroje a techniky	ano	1
6.10	Firewall	ano	1
6.11	Nástroj pro vyhodnocování bezpečnostních událostí (Security Information and Event Management)	ano	1
7	Byly interní systémy organizace účastníka v posledních 12ti měsících podrobeny penetračnímu testování?	ne	0
<b>Část IV. – Zvládání kybernetických incidentů</b>			
8	Má organizace účastníka zaveden proces zvládání kybernetických incidentů?	ano	1
9	Jsou všichni zaměstnanci organizace účastníka pravidelně (min. 1x ročně) vzdělávání v identifikaci kybernetických incidentů?	ano	1
<b>ČÁST V. – Komunikace a vzdělávání</b>			
10	Má organizace účastníka zaveden proces vzdělávání a zvyšování povědomí o kybernetické bezpečnosti zaměstnance?	ano	1
11	Jsou noví zaměstnanci organizace účastníka vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům?	ano	1
12	Vede organizace účastníka přehled vzdělávání a školení zaměstnanců za účelem zlepšení povědomí o kybernetické bezpečnosti zaměstnanců?	ano	1
<b>Celkový bodový součet</b>			<b>63</b>

.....  
 (podpis osoby oprávněné zastupovat jménem či za účastníka, případně razítko)