Příloha 7 – Činnosti podpory bezpečnosti ADIS a bezpečnostní požadavky

1 ČINNOSTI PODPORY BEZPEČNOSTI ADIS

Dodavatel bude realizovat činnosti podpory bezpečnosti ADIS v rozsahu (počet člověkodnů) dohodnutém v příslušné Prováděcí smlouvě.

Činnosti podpory bezpečnosti ADIS budou zahrnovat zejména:

- podporu při vytváření souvisejících metodik, návrhů procesů a analýz,
- aktualizaci bezpečnostní dokumentace ADIS, aktualizace politiky řízení kontinuity činností a havarijního plánu v návaznosti na vývoj Aplikace ADIS
- řízení bezpečnostních incidentů,
- spolupráci při testování nových modulů Aplikace ADIS,
- konzultace k implementaci bezpečnostních opatření,
- účast na jednání týmu bezpečnosti ADIS Zadavatele,
- zpracování/aktualizace plánu zvládání rizik vyplývajícího z analýzy rizik,
- koordinační služby v oblasti bezpečnosti,
- účast na jednání GS AO BEZP, na vyžádání zadavatele,
- ostatní související činnosti v oblasti bezpečnosti ADIS.

2 ZÁKLADNÍ BEZPEČNOSTNÍ POŽADAVKY

Tato příloha popisuje bezpečnostní požadavky Smlouvy o dílo, zejména pro naplnění požadavků vyplývající se zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZOKB"), 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 (dále jen „VKB")) pro prvek kritické informační infrastruktury.

Další požadavky na Zadavatele a Dodavatele související s ochranou osobních údajů vyplývají z nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů (dále jen „GDPR")) a souvisejících právních předpisů.

Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků ZOKB, VKB, zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, GDPR či souvisejících právních předpisů z oblasti bezpečnosti informací či ochrany osobních údajů, uzavřou bez zbytečného odkladu po výzvě kterékoli smluvní strany písemný dodatek Smlouvy zohledňující takové požadavky.

2.1 OPRÁVNĚNÍ UŽÍVAT DATA

a) Dodavatel je při poskytování plnění pro Zadavatele oprávněn užívat data předaná Dodavateli Zadavatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.

b) Dodavatel se při poskytování plnění pro Zadavatele zavazuje nakládat s daty (včetně osobních údajů) pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména GDPR, ZOKB, VKB a dalšími souvisejícími právními předpisy.

2.2 ŘETĚZENÍ A ŘÍZENÍ DODAVATELŮ

a) Dodavatel nezapojí do poskytování plnění dle této Smlouvy (vč. zpracování osobních údajů na základě této Smlouvy) žádného dalšího poddodavatele (v případě osobních údajů zpracovatele) bez předchozího konkrétního nebo obecného povolení Zadavatele;

b) Dodavatel se zavazuje, že se bude řídit požadavky Zadavatele na řízení bezpečnosti informací a poskytne Zadavateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění poddodavatele, zajistí, že bude Zadavateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů;

c) Dodavatel je povinen předat Zadavateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení;

d) pokud Dodavatel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající z této Smlouvy. Dodavatel se zavazuje bezodkladně doložit Zadavateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky vyplývajícími z této Smlouvy;

e) Dodavatel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této Smlouvy; v případě, že dojde k nedodržení těchto požadavků ze strany poddodavatele Dodavatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Dodavatele dle této Smlouvy.

2.3 FYZICKÁ OCHRANA A BEZPEČNOST PROSTŘEDÍ

a) Dodavatel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty technologických a komunikačních systémů, anebo datové nosiče (dále také jen „Pracoviště").

b) Dodavatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k předmětu plnění dle této Smlouvy.

c) Dodavatel se zavazuje v maximální možné míře chránit informace přenášené na přenosným a vyjímatelných médiích. Přenos informací na těchto médiích bude možný pouze v případě zajištění bezpečného šifrování dat na daném médiu.

2.4 MONITOROVÁNÍ ČINNOSTÍ

a) Dodavatel bere na vědomí, že veškerá aktivita Dodavatele a jeho plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související budou Zadavatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy a interních dokumentů Zadavatele.

b) Dodavatel se zavazuje, že bude průběžně monitorovat a zaznamenávat veškerou svoji aktivitu a plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související. Dodavatel je povinen předkládat Zadavateli záznamy/logy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do ICT systému a záznamy o správě uživatelů prováděná na straně Dodavatele, a to v pravidelných intervalech vždy k 15. dni příslušného kalendářního měsíce, nebo kdykoli bez zbytečného odkladu po vyžádání ze strany Zadavatele, a to po celou dobu trvání Smlouvy a i ve vztahu k jejímu ukončení.

2.5 PŘEDÁNÍ A PŘEVZETÍ PLNĚNÍ

a) Dodavatel se zavazuje dodržovat Bezpečnostní požadavky i při předání a převzetí plnění dle této Smlouvy.

b) Zadavatel je oprávněn z důvodu nedodržení Bezpečnostních požadavků včetně požadavku na předání Bezpečnostní dokumentace odmítnout převzetí (části) plnění Smlouvy.

2.6 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

a) Při zpracování osobních údajů zaměstnanců Zadavatele a dalších osob (dále jen „Subjekty údajů") vystupuje Zadavatel jako správce a Dodavatel jako zpracovatel či další zpracovatel (dle konkrétních kategorií údajů a konkrétního obchodního případu), a to za podmínek uvedených níže v tomto článku Smlouvy.

b) Při zpracování osobních údajů je Dodavatel povinen dodržovat veškeré výše uvedené obecné bezpečnostní požadavky vyplývající z této Smlouvy, jakož i požadavky týkající se výhradně zpracování a ochrany osobních údajů.

c) Pokud vznikne potřeba, Zadavatel pověří Dodavatele zpracováním osobních údajů Subjektů údajů poskytovaných Zadavatelem v rámci plnění Smlouvy. Dodavatel je potom povinen zpracovávat

osobní údaje pro Zadavatele na základě jeho doložených pokynů a v rozsahu nezbytném k řádnému plnění povinností Dodavatele vyplývajících ze Smlouvy.

3 POŽADAVKY NA BEZPEČNOST POSKYTOVANÉHO PLNĚNÍ

Při poskytování jednotlivých plnění dle Smlouvy, při poskytování služeb pro zajištění provozu Systému ADIS a při realizaci vývoje Aplikace ADIS bude Dodavatel postupovat zejména v souladu s dále uvedenými bezpečnostními požadavky:

3.1 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Poskytnuté plnění musí být plně v souladu s legislativou, zejména se zákonem 181/2014 Sb. o kybernetické bezpečnosti (ZOKB), vyhláškou 82/2018 Sb. o kybernetické bezpečnosti (VKB). Musí být splněny všechny jejich požadavky včetně zpracování relevantní dokumentace. Musí být v souladu s aktuálně platnými normami řady ISO/IEC 27000.

Dodavatel popíše dopad integrace nových modulů/subsystému ADIS do Systému řízení bezpečnosti informací Zadavatele i dopad na procesy řízení IT služeb (dále „ITSM") Zadavatele ovlivňující úroveň bezpečnosti a kvalitu IT služeb.

3.2 ŘÍZENÍ AKTIV

Výstup vývoje Aplikace ADIS musí splňovat požadavky na řízení aktiv. Dodavatel vydefinuje kategorie dodaných i dotčených aktiv včetně vazeb mezi nimi. Dodavatel zajistí hodnocení aktiv ve smyslu VKB. Dodavatel ve spolupráci se Zadavatelem zajistí aktualizaci evidence aktiv.

3.3 ŘÍZENÍ RIZIK

Dodavatel provede analýzu rizik souvisejících s dodaným vývojem Aplikace ADIS, včetně vlivů souvisejících podpůrných systémů/komponent a včetně zohlednění požadavků GDPR.

3.4 ORGANIZAČNÍ BEZPEČNOST

V rámci výměny informací mezi členy realizačního týmu dodavatel ve spolupráci se Zadavatelem zavede klasifikace informací. Na základě této klasifikace se bude oběh dokumentů a dalších materiálů řídit. Informace budou klasifikovány v úrovních Citlivá, Interní, Veřejná.

Pro efektivní řízení projektu bude ze strany dodavatele navržena komunikační matice s definicí RASCI odpovědností.

3.5 BEZPEČNOSTNÍ ROLE

Dodavatel v souladu s poskytováním služeb a rozsahem vývoje Aplikace ADIS specifikovaným v příslušné Prováděcí smlouvě ustanoví bezpečnostní role ve smyslu ZOKB a VKB.

3.6 ŘÍZENÍ DODAVATELŮ

Dodavatel se zavazuje, že se při poskytování služeb se bude řídit požadavky Zadavatele na řízení bezpečnosti informací a že v celém životním cyklu vývoje Aplikace ADIS poskytne součinnost Zadavateli v otázkách řízení bezpečnosti informací.

3.7 BEZPEČNOST LIDSKÝCH ZDROJŮ

Dodavatel připraví a zajistí poučení svých poddodavatelů o bezpečnostních pravidlech, jež se musí v průběhu poskytování služeb dodržovat a zajistí jejich dodržování nasazením kontrolních a vynucovacích mechanismů. Rozsah poučení bude schvalovat Zadavatel.

3.8 ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

Součástí specifikace vývoje Aplikace ADIS v příslušné Prováděcí smlouvě bude napojení na nástroj pro detekci a vyhodnocení bezpečnostních událostí (SIEM) minimálně v souladu s VKB. Vývoj Aplikace ADIS bude navržen tak, aby byl systém detekce a zvládání bezpečnostních událostí a incidentů začleněn do procesů a systémů Zadavatele.

3.9 AUDIT KYBERNETICKÉ BEZPEČNOSTI

Dodavatel musí souhlasit s provedením auditu ve smyslu ZOKB a VKB, tento strpět a poskytne maximální možnou součinnost při provádění auditních činností Zadavateli nebo osobě pověřené Zadavatelem.

3.10 SPRÁVA A OVĚŘOVÁNÍ IDENTIT

Řízení přístupu bude vycházet ze standardu normy ISO/IEC/27002. Striktně musí být omezeno používání technologických (nepersonalizovaných) účtů, a to pouze na případy, kdy je to nezbytně nutné z technologického hlediska.

3.11 OCHRANA PŘED ŠKODLIVÝM KÓDEM

Řešení musí být připraveno integrovat ochranu před škodlivým kódem Zadavatele tak, aby byla zajištěna bezpečnost datových objektů, a to jak směrem k externímu uživateli, tak k pracovníkům Zadavatele, navazujícím integrovaným systémům, podpůrným systémům, ale i v rámci zajištění persistence dat (uložení v databázi).

3.12 APLIKAČNÍ BEZPEČNOST

Před spuštěním nového modulu/subsystémy Aplikace ADIS do rutinního provozu proběhne v gesci Zadavatele penetrační testování řešení 3. stranou. Nálezy vyplývající z testování kategorie medium a výše budou řešeny na náklady Dodavatele.

3.13 KRYPTOGRAFICKÉ PROSTŘEDKY

Dodavatel použije pouze aktuálně odolné kryptografické algoritmy a kryptografické klíče, bude se řídit doporučenými kryptografickými metodami minimálně podle ZOKB a VKB.

3.14 ZAJIŠŤOVÁNÍ ÚROVNĚ DOSTUPNOSTI INFORMACÍ

Nové moduly/subsystémy Aplikace ADIS (architektura z pohledu HA/LB/DR) musí dosahovat očekávané RPO/RTO/SLA. Prokázání deklarované dostupnosti před předáním plnění Zadavateli bude realizováno protokoly z testovacího obnovení prostředí s naplněním RPO/RTO. Webové části řešení musí být chráněny proti známým útokům, které byly identifikovány a dokumentovány podle OWASP.

3.15 SPECIFICKÉ POŽADAVKY SOUVISEJÍCÍ S NAPLNĚNÍM GDPR

V souvislosti s požadavky regulace GDPR je nezbytné nad rámec výše uvedených požadavků zajistit důslednou auditní stopu pro veškeré operace prováděné nad osobními údaji subjektů. Tyto záznamy by měly být ideálně odděleny od běžné transakční/provozní historie a měly by mít zvláštní režim (uchování, přístupu na uvedené záznamy apod.).