Evidenční číslo smlouvy: 0545/2025/OIKT/1050

SMLOUVA O DÍLO NA KONFIGURACE A IMPLEMENTACE BEZPEČNOSTNÍCH FUNKCÍ PROSTŘEDÍ MICROSOFT

SMLUVNÍ STRANY:

Obchodní jméno:	**Městská část Praha 14**
se sídlem:	Bratří Venclíků 1073, Černý Most, 198 00 Praha
IČO:	002 31 312

(dále jen „**Objednatel**“)

a

Obchodní jméno:	**Aricoma Systems a.s.**
se sídlem:	Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava
IČO:	04308697
DIČ:	CZ04308697
zápis v OR:	B 11012 vedená u Krajského soudu v Ostravě
zastoupená:	Ing. Vítem Ševčíkem, členem představenstva

(dále jen „**Dodavatel**“)

(Objednatel a Dodavatel dále společně jen „**Smluvní strany**“ nebo jednotlivě „**Smluvní strana**“)

dnešního dne uzavřely v souladu s ustanovením § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“) tuto Smlouvu (dále jen „**Smlouva**“)

1. PREAMBULE

1.1 Tato Smlouva je uzavírána na základě zadávací dokumentace veřejné zakázky malého rozsahu s názvem „KONFIGURACE A IMPLEMENTACE BEZPEČNOSTNÍCH FUNKCÍ PROSTŘEDÍ MICROSOFT“ včetně všech jejich příloh (dále jen „**Veřejná zakázka**“), zadávací dokumentace je ke dni uzavření Smlouvy dostupná na profilu Objednatele jako zadavatele.

1.2 Objednatel prohlašuje, že splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené. Objednatel dále prohlašuje, že má zájem na uzavření této Smlouvy s odborníkem v oboru informačních technologií s dostatečnými zkušenostmi a know-how v oblasti realizace Veřejné zakázky za podmínek dále stanovených v této Smlouvě.

1.3 Dodavatel prohlašuje, že se detailně seznámil s rozsahem a povahou plnění dle Veřejné zakázky, a to tak, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k realizaci této Smlouvy a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci této Smlouvy za dohodnuté smluvní ceny uvedené ve Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění Veřejné zakázky.

2. ÚČEL SMLOUVY

2.1 Základním účelem, pro který se Smlouva uzavírá, je realizace Veřejné zakázky dle zadávacích podmínek, tedy zejména provedení díla spočívajícího zejména v provedení konfigurace a implementace bezpečnostních funkcí prostředí Microsoft, tj. zejména kompletní instalace a implementace v prostředí, včetně zajištění napojení na další systémy v souladu se standardy, konfigurace a implementace správy privilegovaných účtů, Just-In-Time (JIT) přidělování práv, pravidelné auditování, zavedení Multi-Factor Authentication (MFA), plné nasazení a zkušební provoz Microsoft Defender for Office 365, Safe Attachments a Safe Links a Data Loss Prevention (DLP) - nastavení pravidel pro zamezení únikům citlivých informací (např. automatické blokace, šifrování).

2.2 Účelem Smlouvy je dále naplnění cílů a realizace části projektu Národního plánu obnovy *„Posílení kybernetické bezpečnosti Úřadu městské části Praha 14“*, registrační číslo projektu: CZ.31.2.0/0.0/0.0/24_145/0011561.

2.3 Dodavatel touto Smlouvou garantuje Objednateli splnění zadání Veřejné zakázky a všech z toho vyplývajících podmínek a povinností podle zadávací dokumentace Veřejné zakázky. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této Smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že:

2.3.1 v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel Veřejné zakázky vyjádřený v zadávacích podmínkách Veřejné zakázky, cíle projektu definované v čl. 2.2 této Smlouvy;

2.3.2 v případě chybějících ustanovení této Smlouvy budou použita dostatečně konkrétní ustanovení zadávacích podmínek Veřejné zakázky;

2.3.3 v případě rozporu ustanovení libovolné Přílohy této Smlouvy s textem uvedeným ve Smlouvě, bude použito ustanovení této Smlouvy.

2.4 Dodavatel je vázán svou nabídkou předloženou Objednateli v rámci zadávacího řízení na zadání Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících z této Smlouvy použije subsidiárně.

3. DEFINICE POJMŮ

3.1 V této Smlouvě jsou používané pojmy uvedené níže.

3.1.1 „**Akceptační protokol**" znamená písemný protokol o předání a převzetí Díla, resp. jeho části, který musí splňovat náležitosti uvedené v čl. 13.5.

3.1.2 „**Akceptační proces**" znamená proces formálního předání a převzetí Díla, resp. jeho části, navazující na Akceptační testy a spočívající v sepsání Akceptačního protokolu a jeho podpisu Smluvními stranami.

3.1.3 „**Akceptační testy**" má význam definovaný v čl. 13.4.1 této Smlouvy.

3.1.4 „**Autorská díla**" má význam definovaný v čl. 15.3 této Smlouvy.

3.1.5 „**Autorský zákon**" má význam definovaný v čl. 15.3 této Smlouvy.

3.1.6 „**Cena Díla**" má význam definovaný v čl. 7.1 této Smlouvy.

3.1.7 „**Dílo**" znamená dílo, jak je definováno v čl. 4.2 této Smlouvy.

3.1.8 „**Důvěrné informace**" má význam definovaný v čl. 19.1.1 této Smlouvy.

3.1.9 „**Faktura**" má význam definovaný v čl. 8.1 této Smlouvy.

3.1.10 „**Harmonogram**" má význam definovaný v čl. 5.2 této Smlouvy.

3.1.11 „**Hodnocení důsledků**" má význam definovaný v čl. 18.2 této Smlouvy.

3.1.12 „**Technická specifikace**" má význam definovaný v čl. 4.1 této Smlouvy.

3.1.13 „**Kybernetické požadavky**" má význam definovaný v čl. 20.3 této Smlouvy.

3.1.14 „**Licence**" má význam definovaný v čl.15.3 této Smlouvy.

3.1.15 „**Milník**" znamená jednotlivé postupové termíny provádění Díla, věcně a časově specifikované v Harmonogramu (Příloha č. 2).

3.1.16 „**Nespolehlivý plátce**" má význam definovaný v čl. 8.9 této Smlouvy.

3.1.17 **Oprávněné osoby**" má význam definovaný v čl. 9.1 této Smlouvy.

3.1.18 „**Oprávněná strana**" má význam definovaný v čl. 16.1 této Smlouvy.

3.1.19 „**Projektová etapa**" znamená jednu nebo více ucelených částí plnění předmětu této Smlouvy dle Přílohy č. 1 a Přílohy č. 2, jejímž cílem je dodání ucelené části Díla Dodavatelem Objednateli.

3.1.20 „**Porušující strana**" má význam definovaný v čl. 16.1 této Smlouvy.

3.1.21 „**Veřejná zakázka**" má význam definovaný v čl. 1.1 této Smlouvy.

3.1.22 „**Vyšší moc**" má význam definovaný v čl. 17.3 této Smlouvy.

3.1.23 „**Zákon o registru smluv**" má význam definovaný v čl. 19.12.6 této Smlouvy.

3.2 **Odkazy.** Odkazy na články nebo Přílohy použité v této Smlouvě jsou odkazy na články a Přílohy této Smlouvy, není-li uvedeno jinak.

3.3 **Záhlaví**. Nadpisy v této Smlouvě slouží pouze jako odkaz a nemají vliv na výklad této Smlouvy.

4. PŘEDMĚT SMLOUVY

4.1 **Předmět smlouvy.** Dodavatel se zavazuje na vlastní náklady a nebezpečí pro Objednatele implementovat řádně a včas a za cenu a podmínek stanovených dále v této Smlouvě, bezpečnostní funkce, jak je blíže specifikováno v Příloze č. 1 Smlouvy (dále jen „**Technická specifikace**“).

4.2 **Plnění Dodavatele.** Plnění podle čl. 4.1 této Smlouvy zahrnuje zejména následující činnosti Dodavatele dle Technické specifikace, které se Dodavatel zavazuje provést zejména:

4.2.1 analýzu a přípravu prostředí Objednatele;

4.2.2 sestavení podrobného harmonogramu realizačních prací;

4.2.3 úprava (customizace) a nastavení informačních systémů Objednatele,

4.2.4 integrace dle čl. 5.1;

4.2.5 zhotovení a dodání programových úprav;

4.2.6 provedení všech dalších odborných implementačních prací, jimiž se rozumí souhrn činností směřujících ke zprovoznění funkčního celku, informačního systému, u Objednatele s daty Objednatele, tedy zejména instalační práce, případné migrace dat, školení, testování, programování, odstraňování chyb bránících akceptaci, konzultace, vypracování technické a provozní dokumentace, jakož i další odborné práce nezbytné k integraci jednotlivých komponent do komplexního funkčního řešení v rozsahu vymezeném na základě této Smlouvy,

a to vše v rozsahu uvedeném v této Smlouvě případně dohodnutém Smluvními stranami v souladu s touto Smlouvou a jejími přílohami (shora uvedené v čl. 4.1 a 4.2 dále jen „**Dílo**“).

4.3 **Plnění Objednatele.** Objednatel se zavazuje poskytovat Dodavateli součinnost v souvislosti s provedením Díla, jak je stanovena v Technické specifikaci, Příloze č. 3 nebo bude dohodnuta v souladu s touto Smlouvou, přebírat Projektové etapy Díla a Dílo jako celek a zaplatit Cenu Díla dle podmínek sjednaných touto Smlouvou a Přílohou č. 7.

5. ZPŮSOB PROVÁDĚNÍ DÍLA

5.1 **Integrace.** V rámci integračních služeb Dodavatel integruje jednotlivé součásti Díla spolu s již existujícími systémy Objednatele podle Technické specifikace.

5.2 **Řízení provádění Díla.** Realizaci Díla řídí a metodicky vede Dodavatel. Popis rozvržení Díla na Projektové etapy je uveden v Technické specifikaci a v Příloze č. 2 (dále jen „**Harmonogram**“). Objednatel se zavazuje poskytnout Dodavateli včasnou součinnost pro řízení implementace uvedenou v Příloze č. 3.

5.3 **Odpovědnost.** Dodavatel je odpovědný za provádění Díla, včetně strategie implementace Díla a návrhu jeho integrace do již existujících systémů Objednatele, Harmonogramu implementace a jednotlivých Projektových etap (včetně detailního procesu implementace), návrhu infrastruktury a aplikační a integrační architektury v průběhu provádění Díla. Dodavatel neodpovídá za činnosti, které jsou odpovědností Objednatele a jednání třetích stran, které nejsou poddodavateli Dodavatele.

5.4 **Školení.** Dodavatel připraví a provede školení pracovníků Objednatele dle Technické specifikace.

5.5 **Administrace Díla**

5.5.1 Dodavatel se zavazuje průběžně informovat (standardně na týdenní bázi) Objednatele o stavu realizace Díla, se zaměřením na operativní aktivity týkající se časového rozvrhu, rozsahu a plánu aktivit a jejich plnění, zejména s důrazem na otevřené problémy a rizika.

5.5.2 Dodavatel se zavazuje, že prostřednictvím svého projektového manažera bude prezentovat souhrnné měsíční zprávy o stavu realizace Díla vedoucímu projektu a managementu Objednatele.

5.5.3 Dodavatel zajistí výstup z každé projektové schůzky, na které je účasten alespoň jeden člen jeho týmu, formou strukturovaného zápisu, případně jinou formou dohodnutou Smluvními stranami. Zápis může po dohodě Smluvních stran doplnit i videonahrávka. Objednatel je povinen se k takovém zápisu vyjádřit do pět (5) pracovních dnů od jeho předložení Dodavatelem. Pokud se k Objednatel k zápisu ve lhůtě dle předchozí věty nevyjádří, má se za to, že s takovým zápisem souhlasí.

5.5.4 Dodavatel se zavazuje pravidelně provádět analýzu rizik a řízení rizikového plánu v souvislosti s plněním této Smlouvy. Veškerá rizika musí být uvedena ve zprávách o stavu, zejména při pravidelném reportingu „stavu Díla“ a před začátkem Projektové etapy. Ke každému riziku bude přiřazeno opatření pro jeho mitigaci a aplikace opatření je vyhodnocována.

6. MÍSTO PLNĚNÍ

6.1 Místem plnění je sídlo Objednatele, tj. Bratří Venclíků 1073, Černý Most, 198 00 Praha případně též jiné prostory dle potřeby a výslovného pokynu Objednatele.

6.2 Pokud to povaha realizace Díla této Smlouvy umožňuje a Objednatel vůči tomu nemá výhrady, je Dodavatel oprávněn provádět relevantní části Díla vzdáleným přístupem.

7. CENA

7.1 **Cena Díla.** Smluvní strany se dohodly, že cena za Dílo je položkově specifikována v Příloze č. 7 (dále jen „**Cena Díla**“).

7.2 Cena Díla bude hrazena postupně v souladu s Harmonogramem uvedeným v Příloze č. 2 této Smlouvy. Každá část Ceny Díla bude splatná po řádném dokončení a akceptaci příslušné Projektové etapy.

7.3 Dodavatel výslovně prohlašuje, že Cena Díla dle Smlouvy již v sobě zahrnuje veškeré náklady Dodavatele spojené s plněním dle této Smlouvy vč. nákladů na dopravu do místa plnění, nákladů na balení, cla, celních poplatků, licenčních a jiných poplatků.

8. PLATEBNÍ PODMÍNKY

8.1 Cenu Díla je Objednatel povinen uhradit Dodavateli na základě daňového dokladu (faktury) (dále jen „**Faktura**“) vystaveného Dodavatelem po akceptaci příslušné Projektové etapy dle jednotlivých Milníků uvedených v Harmonogramu (viz Příloha č. 2). Přílohou každé Faktury musí být kopie podepsaného Akceptačního protokolu.

8.2 Splatnost jednotlivých Faktur se sjednává na třicet (30) dnů ode dne jejich doručení povinné Smluvní straně. Toto ustanovení se uplatní i v případě hrazení smluvních pokut.

8.3 Všechny Faktury musí splňovat náležitosti řádného daňového dokladu požadované § 435 Občanského zákoníku a zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a vždy musí výslovně obsahovat následující údaje: označení Smluvních stran a jejich adresy, IČO, DIČ (je-li přiděleno), údaj o tom, že vystavovatel Faktury je zapsán v obchodním rejstříku včetně spisové značky, označení této Smlouvy, označení poskytnutého plnění, označení registračního čísla dotačního projektu (CZ.31.2.0/0.0/0.0/24_145/0011561), jeho rozsah, jednotkovou a celkovou cenu, číslo Faktury, den vystavení a lhůtu splatnosti Faktury, označení peněžního ústavu a číslo účtu, na který se má platit, fakturovanou částku, razítko a podpis Oprávněné osoby. Faktura bude vždy obsahovat příslušné dodací listy, Akceptační protokoly vztahující se k jednotlivým částem Díla a jiné přílohy požadované Objednatelem. Faktury budou znít na částku v české měně (Kč).

8.4 Nebude-li Faktura obsahovat stanovené náležitosti a přílohy, nebo v ní nebudou správně uvedené údaje dle této Smlouvy, je Objednatel oprávněn vrátit ji ve lhůtě její splatnosti Dodavateli. V takovém případě se přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené Faktury.

8.5 Platby peněžitých částek se provádí bankovním převodem na účet druhé Smluvní strany uvedený ve Faktuře. Peněžitá částka se považuje za zaplacenou okamžikem jejího odepsání z účtu odesílatele ve prospěch účtu příjemce.

8.6 Objednatel neposkytuje Dodavateli na předmět plnění této Smlouvy jakékoliv zálohy.

8.7 V případě prodlení kterékoliv Smluvní strany se zaplacením peněžité částky vzniká oprávněné Smluvní straně nárok na úrok z prodlení v zákonné výši dlužné částky za každý i započatý den prodlení. Tím není dotčen ani omezen nárok na náhradu vzniklé újmy.

8.8 Objednatel bude hradit přijaté Faktury pouze na bankovní účty Dodavatele zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona o DPH. V případě, že Dodavatel nebude mít svůj bankovní účet tímto způsobem zveřejněn, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH uhradí Dodavateli až po zveřejnění příslušného účtu Dodavatele v registru plátců a identifikovaných osob Dodavatelem.

8.9 Dodavatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že Dodavatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „**nespolehlivý plátce**“). V případě, že správce daně rozhodne o tom, že Dodavatel je nespolehlivým plátcem, zavazuje se Dodavatel o tomto informovat Objednatele do dvou (2) pracovních dní. Stane-li se Dodavatel nespolehlivým plátcem, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH bude Objednatelem uhrazena Dodavateli až po písemném doložení Dodavatele o jeho úhradě této DPH příslušnému správci daně.

9. OPRÁVNĚNÉ OSOBY A ŘÍZENÍ PROVÁDĚNÍ DÍLA

9.1 **Oprávněné osoby.** Každá ze Smluvních stran jmenuje oprávněné osoby nebo jejich zástupce, kteří ji zastupují v záležitostech týkajících se předmětu této Smlouvy (dále jen „**Oprávněné osoby**“). Pověření zástupce k zastupování Oprávněné osoby musí být písemné a musí v něm být uveden rozsah tohoto pověření. Aktuální seznam Oprávněných osob jmenovaných Smluvními stranami je připojen jako Příloha č. 5 této Smlouvy.

10. POVINNOSTI DODAVATELE

10.1 **Povinnosti Dodavatele.** Dodavatel se zavazuje:

10.1.1 sestavit v součinnosti s Objednatelem detailní harmonogram celé realizace Díla, který bude vycházet z úvodního harmonogramu, jak je uveden v Harmonogram, a detailní harmonogram si nechat písemně odsouhlasit Objednatelem;

10.1.2 předávat Dílo (nebo jeho část) k Akceptačnímu procesu tak, aby mohlo být v termínech stanovených v Harmonogramu řádně akceptováno v souladu s čl. 13 této Smlouvy;

10.1.3 odstranit ve sjednaných lhůtách jakékoli vady, jež má Dílo či jeho část k okamžiku akceptace;

10.1.4 neprodleně oznámit Objednateli jakékoli překážky, které mu brání v provádění Díla a výkonu dalších činností souvisejících s plněním předmětu Smlouvy;

10.1.5 upozornit Objednatele na potenciální rizika vzniku škod a provést včas a řádně na své náklady taková opatření, které riziko sníží nebo zcela vyloučí;

10.1.6 upozorňovat Objednatele v odůvodněných případech na případnou nevhodnost pokynů Objednatele;

10.1.7 i bez pokynů Objednatele provést nutné úkony, které, ač nejsou předmětem této Smlouvy, budou s ohledem na nepředvídatelné okolnosti pro plnění Smlouvy nezbytné nebo jsou nezbytné pro zamezení vzniku škody;

10.1.8 dodržovat bezpečnostní, hygienické, požární, organizační a ekologické předpisy Objednatele, se kterými byl prokazatelně seznámen nebo které jsou všeobecně známé;

10.1.9 řešit písemné požadavky či dotazy Objednatele vztahující se k předmětu plnění dle této Smlouvy, a to nejpozději ve lhůtě pěti (5) pracovních dnů ode dne jejich doručení Dodavateli.

10.2 Dodavatel se zavazuje po celou dobu trvání smluvního vztahu založeného Smlouvou zajistit dodržování veškerých právních předpisů, zejména pak pracovněprávních (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy), dále předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů, a to vůči všem osobám, které se na plnění Smlouvy podílejí (a bez ohledu na to, zda budou činnosti prováděny Dodavatelem či jeho poddodavateli). Dodavatel se také zavazuje zajistit, že všechny osoby, které se na plnění Smlouvy podílejí (bez ohledu na to, zda budou činnosti prováděny Dodavatelem či jeho poddodavateli), jsou vedeny v příslušných registrech, jako například v registru pojištěnců ČSSZ, a mají příslušná povolení k pobytu v ČR.

10.3 Dodavatel je dále povinen zajistit, že všechny osoby, které se na plnění Smlouvy podílejí (bez ohledu na to, zda budou činnosti prováděny Dodavatelem či jeho poddodavateli) budou proškoleny z problematiky BOZP, a že jsou vybaveny osobními ochrannými pracovními prostředky dle účinné legislativy, je-li používání osobních ochranných pracovních prostředků s ohledem na předmět plnění Smlouvy vyžadováno. V případě, že Dodavatel (či jeho poddodavatel) bude v rámci řízení zahájeného dle tohoto odstavce Smlouvy orgánem veřejné moci pravomocně uznán vinným ze spáchání přestupku, správního deliktu či jiného obdobného protiprávního jednání, je Dodavatel povinen přijmout nápravná opatření

a o těchto, včetně jejich realizace, písemně informovat Objednatele, a to v přiměřené lhůtě stanovené po dohodě s Objednatelem. Objednatel je oprávněn odstoupit od této Smlouvy, pokud Dodavatel nebo jeho poddodavatel bude orgánem veřejné moci uznán pravomocně vinným ze spáchání přestupku či správního deliktu, popř. jiného obdobného protiprávního jednání, v řízení dle tohoto odstavce Smlouvy.

10.4 Dodavatel musí po celou dobu trvání Smlouvy sjednat a dodržovat obdobné smluvní podmínky v oblasti rozdělení rizika a smluvních pokut se svými poddodavateli s ohledem na charakter, rozsah a cenu plnění poddodavatele, jako jsou sjednané v této Smlouvě.

10.5 Dodavatel se v rámci svých vnitřních procesů zavazuje k podpoře firemní kultury založené na motivaci pracovníků k zavádění inovativních prvků, procesů či technologií v rámci tzv. Best Practices.

10.6 Dodavatel se zavazuje plnění dle této Smlouvy poskytovat sám nebo s využitím poddodavatelů uvedených v Příloze č. 4 této Smlouvy. Jakákoliv dodatečná změna osoby poddodavatele nebo rozsahu plnění svěřeného poddodavateli musí být předem písemně oznámena Objednateli, ledaže by plnění původně svěřené poddodavateli realizoval Dodavatel sám. Změna osoby poddodavatele, kterým byla prokazována kvalifikace v rámci zadávacího řízení Veřejné zakázky, nebo rozsahu plnění Smlouvy, který má takový poddodavatel vykonávat, musí být předem schválena Objednatelem. Objednatel takovou změnu neodmítne v případě, že nový poddodavatel bude disponovat přinejmenším kvalifikací na stejné úrovni, která byla prokazována původním poddodavatelem v zadávacím řízení Veřejné zakázky. Uvedené skutečnosti je Dodavatel povinen Objednateli prokázat způsobem odpovídajícím prokazování kvalifikace v zadávacím řízení Veřejné zakázky.

10.7 Dodavatel se zavazuje alokovat na provádění Díla dle této Smlouvy kapacity členů realizačního týmu Dodavatele a provádět Dílo dle Smlouvy za účasti členů realizačního týmu uvedeného v Příloze č. 4 této Smlouvy, jimiž Dodavatel prokázal svou kvalifikaci v rámci Veřejné zakázky. Alokací kapacity se rozumí dostupnost kteréhokoliv člena realizačního týmu nebo jeho odpovídajícího náhradníka, jenž má minimálně stejnou kvalifikaci jako nahrazovaný člen. Jakákoliv dodatečná změna členů realizačního týmu musí být předem projednána a písemně schválena Objednatelem, přičemž změna bude Objednatelem schválena v případě, že Dodavatel nahradí osobu realizačního týmu takovou osobou, která prokazatelně disponuje znalostmi a odbornou kvalifikací alespoň na úrovni, která byla u nahrazované osoby předmětem posouzení.

11. ODPOVĚDNOST ZA VADY

11.1 Dodavatel poskytuje záruku, že každá část Díla má ke dni její akceptace funkční vlastnosti stanovené touto Smlouvou a je způsobilé k použití pro účely stanovené v této Smlouvě nebo v souladu s touto Smlouvou.

11.2 Dodavatel poskytuje záruku za jakost k Dílu/jeho části od okamžiku jeho akceptace po dobu dvou (2) let od akceptace.

11.3 Objednatel je oprávněn vady Díla nahlásit Dodavateli kdykoli v průběhu záruční doby bez ohledu na to, kdy je zjistil, aniž by tím byla jeho práva ze záruky či práva z vad jakkoli dotčena.

11.4 Doba od zjištění vady do jejího odstranění se do trvání záruční doby nezapočítává.

11.5 Dílo má vady, zejména pokud nebylo poskytnuto v souladu s Technickou specifikací.

11.6 V případě, že je dodáno Dílo s vadami, či se na Díle vady v záruční době vyskytnou, je Dodavatel povinen vady odstranit opravou či pokud Objednatel takový požadavek uvede v oznámení vad, přiměřenou slevou z Ceny Díla.

11.7 Nároky z vad Díla se nedotýkají nároku Objednatele na náhradu újmy nebo na smluvní pokutu.

12. TERMÍNY PLNĚNÍ

12.1 **Termín plnění.** Dodavatel provede Dílo v termínech dle Harmonogramu.

13. PŘEDÁNÍ DÍLA – AKCEPTAČNÍ PROCES

13.1 **Dílčí části.** Ustanovení čl. 13 této Smlouvy o předání a převzetí Díla se vztahují rovněž na předání a převzetí části Díla, zejména Projektových etap, není-li výslovně stanoveno jinak, jakož i vzniku nároku na zaplacení odpovídajícím částem Ceny Díla.

13.2 **Zaplacení Ceny Díla.** Řádně předaným a převzatým Dílem se rozumí Dílo, které bylo akceptováno Objednatelem v Akceptačním procesu a byl o něm vyhotoven Akceptační protokol, případně se považuje za akceptované dle čl. 13.4.8 nebo 13.4.12 této Smlouvy. Akceptace Díla Objednatelem je podmínkou pro vznik nároku na zaplacení Ceny Díla.

13.3 **Předložení Díla**. Dodavatel nejméně dva (2) pracovní dny před předložením Díla k akceptaci písemně vyzve Objednatele k zahájení testování na straně Objednatele tak, aby Dílo mohlo být při řádné součinnosti Objednatele akceptováno v termínu pro dokončení Díla dle Harmonogramu.

13.4 **Akceptace Díla a jeho částí.**

13.4.1 Akceptace Díla a jeho částí (Projektových etap), bude provedena formou akceptačních testů (dále jen „**Akceptační testy**“) a zakončena Akceptačním procesem.

13.4.2 Dodavatel se zavazuje otestovat funkčnost Díla sám v souladu se strategií testování a způsobem uvedeným v Technické specifikaci.

13.4.3 Dodavatel se zavazuje předat k Akceptačním testům Dílo v souladu se strategií testování a způsobem uvedeným v Technické specifikaci.

13.4.4 Dílo nebo jeho část má vady, pokud nesplňuje požadavky dle Technické specifikace nebo není použitelné k účelu Smlouvy. Nesplnění Akceptačního testu se považuje za nesoulad s Technickou specifikací.

13.4.5 Akceptační testy provádí Objednatel, k čemuž mu Dodavatel poskytne veškerou potřebnou součinnost.

13.4.6 Vady budou kategorizovány dle následující pravidel:

Kategorie vady / (Označení Objednatele)	Popis vady
A (1)	- Nefunkční prioritní proces/core funkcionalita a neexistuje workaround. - Není alternativa – testování na úrovni jedné či více komponent nemůže pokračovat – blokuje testy.

Kategorie vady / (Označení Objednatele)	Popis vady
B (2)	- Nefunkční prioritní proces/core funkcionalita, kde existuje v aplikaci workaround. - Může být takto kategorizován i defekt, na kterém neexistuje workaround, ale impactuje velkou množinu testů dané funkcionality, ovšem není celkově, tak kritický, aby byl označen jako blocker.
C (3-4)	- Chyba v neprioritním procesu/funkčnosti - Chyba vyskytující se pouze při určitých podmínkách či použitých vstupních datech.
D (5-6)	- Ostatní vady.

13.4.7 Kategorii vady navrhuje oprávněná osoba Objednatele a potvrzuje oprávněná osoba Dodavatele v odezvě na vadu. V případě jakéhokoli sporu rozhoduje Objednatel.

13.4.8 Objednatel je povinen Dílo nebo jeho část akceptovat, pokud nevykazuje žádnou vadu kategorie A a B a současně maximálně 20 vad kategorie C. Smluvní strany se mohou při akceptaci dohodnout i jinak. Objednatel se zavazuje akceptovat (převzít) Dílo či jeho část, nebo sdělit Dodavateli vady nejpozději do tří (3) pracovních dnů od předložení Díla či jeho části k Akceptačnímu procesu, nebude-li v konkrétním případě dohodnuto jinak. Pokud Objednatel ve lhůtě dle předchozí věty nesdělí Dodavateli vady Díla či jeho části nebo z objektivních důvodu nepožádá o prodloužení lhůty, má se za to, že Dílo či jeho předmětnou část akceptoval.

13.4.9 Bude-li Dílo nebo jeho část akceptována s vadami, nebo pokud nebude akceptována, uvedou k tomuto Smluvní strany do Akceptačního protokolu svá stanoviska a budou postupovat dle vzájemné dohody a v souladu s čl.13.4 této Smlouvy.

13.4.10 Po odstranění vad kategorie A a B nebo nadlimitního počtu vad kategorie C se Akceptační proces opakuje. V případě, že Dílo nebo jeho část překračuje k termínu jednotlivého Milníku maximální počet vad stanovený pro splnění akceptačních kritérií, je Dodavatel v prodlení. Opakovaně (opakovaně znamená třetí a další kolo Akceptačního procesu) neúspěšný Akceptační proces stejné části Díla (tj. část Díla, která je předmětem Akceptačního procesu překračuje na konci Akceptačního procesu maximální počet vad stanovený pro splnění akceptačních kritérií) je podstatným porušením Smlouvy Dodavatelem.

13.4.11 Dílo jako celek se považuje za dokončené, bylo-li řádně převzato Objednatelem, tedy pokud došlo k protokolárnímu převzetí všech částí Díla dané Projektové etapy na základě příslušných Akceptačních protokolů nebo se považuje za akceptované dle čl. 13.4.8 a 13.4.12 této Smlouvy.

13.4.12 Bez ohledu na ostatní ustanovení tohoto čl. 13 a pokud se Smluvní strany nedohodou jinak se má za to, že Objednatel řádně převzal Dílo, pokud Objednatel užívá Dílo v komerčním provozu.

13.5 **Akceptační protokol.** Akceptační protokol bude obsahovat zejména:

13.5.1 identifikaci Smlouvy;

13.5.2 předmět akceptace (Dílo/část Díla, které se Akceptační protokol týká);

13.5.3 obsah akceptace (co bylo v rámci Akceptačního procesu předáno);

13.5.4 informaci o tom, zda bylo Dílo nebo jeho část:

a) akceptován bez výhrad;

b) akceptován s výhradami; nebo

c) neakceptován.

13.5.5 v případě akceptace s výhradami/neakceptace, popis výhrad (vad), jejich množství a závažnost;

13.5.6 datum zahájení Akceptačního procesu a datum předání Díla či jeho části;

13.5.7 vzor Akceptačního protokolu je Přílohou č. 8 Smlouvy.

14. PODPORA

14.1 Dodavatel se zavazuje Objednateli poskytovat podporu Díla v rozsahu a po dobu, které jsou blíže určeny v Technické specifikaci.

15. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA

15.1 V případě, že součástí Díla Dodavatele podle této Smlouvy jsou věci, které se mají stát vlastnictvím Objednatele, nabývá Objednatel vlastnické právo k těmto věcem dnem předání takového plnění Objednateli na základě Akceptačního protokolu podepsaného oprávněnými osobami obou Smluvních stran. Nebezpečí škody na předaných věcech přechází na Objednatele okamžikem jejich faktického předání do dispozice Objednatele, pokud o takovém předání byl sepsán písemný záznam podepsaný oprávněnými osobami Smluvních stran.

15.2 Do okamžiku nabytí vlastnického práva uděluje Dodavatel Objednateli právo Dílo/či jeho část (ke které se uděluje vlastnické právo) užívat v rozsahu a způsobem, jenž vyplývá z účelu této Smlouvy, a to bez vzniku jakýchkoliv dodatečných finančních nároků nad rámec ceny sjednané v této Smlouvě. Užití tohoto plnění nezpůsobuje fikci převzetí plnění ani podpisu akceptace.

15.3 Vzhledem k tomu, že součástí Díla dle této Smlouvy je i plnění, které ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**Autorský zákon**“), může naplňovat znaky autorského díla či být považováno za autorské dílo ve smyslu autorského zákona (dále společně jen „**Autorská díla**“), je k tomuto plnění poskytována, postupována či zprostředkovávána licence či podlicence (dále společně jen „**Licence**“) za podmínek sjednaných dále v tomto článku Smlouvy.

15.3.1 Objednatel je oprávněn od okamžiku účinnosti poskytnutí Licence k autorskému dílu dle této Smlouvy užívat toto Autorské dílo k jakémukoliv účelu a v rozsahu, v jakém uzná za nezbytné, vhodné či přiměřené. Pro vyloučení pochybností to znamená, že Objednatel je oprávněn užívat Autorské dílo v neomezeném množstevním a územním rozsahu, a to všemi v úvahu přicházejícími způsoby a s

časovým rozsahem omezeným pouze dobou trvání majetkových autorských práv k takovémuto Autorskému dílu.

15.3.2 Licence k Autorskému dílu je poskytována jako nevýhradní. Objednatel není povinen Licenci využít.

15.3.3 Účinnost Licence nastává okamžikem akceptace dílčího plnění, které příslušné Autorské dílo obsahuje; do té doby je Objednatel oprávněn Autorské dílo užít v rozsahu a způsobem nezbytným k provedení akceptace příslušného dílčího plnění.

15.3.4 Udělení Licence nelze ze strany Dodavatele do doby trvání této Smlouvy vypovědět a její účinnost trvá minimálně po dobu trvání této Smlouvy, nedohodnou-li se Smluvní strany výslovně jinak.

15.3.5 Pro vyloučení veškerých pochybností Smluvní strany výslovně prohlašují, že pokud při provedení Díla dle této Smlouvy vznikne činností Dodavatele a Objednatele dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, platí, že k okamžiku vzniku takového díla spoluautorů postoupil Dodavatel Objednateli právo vykonávat majetková autorská práva k dílu spoluautorů a udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena Díla je stanovena se zohledněním tohoto ustanovení a Dodavateli nevzniknou v případě vytvoření díla spoluautorů žádné nové nároky na odměnu.

15.3.6 Dodavatel je povinen postupovat tak, aby udělení Licence k Autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci a souvisejících oprávnění zabezpečil, a to bez újmy na právech třetích osob.

15.4 Součástí plnění může být tzv. proprietární (standardní) software anebo tzv. open source software Dodavatele nebo třetích stran (dále společně jen **„standardní software**“) u kterých Dodavatel nemůže udělit Objednateli Licenci v rozsahu dle čl. 15.3 Smlouvy nebo to po něm nelze spravedlivě požadovat, pouze při splnění některé z následujících podmínek (pro vyloučení veškerých pochybností Smluvní strany uvádí, že v případě, kdy je vývoj počítačového programu hrazen Objednatelem na základě této Smlouvy, může Objednatel vždy požadovat udělení oprávnění dle čl. 15.3 Smlouvy):

15.4.1 Jedná se o software, který je v době uzavření Smlouvy prokazatelně užíván v produktivním prostředí nejméně u pěti (5) na sobě nezávislých a vzájemně nepropojených subjektů a jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň třemi (3) na sobě nezávislými a vzájemně nepropojenými subjekty:

a) pokud jsou tyto subjekty oprávněny takovýto software implementovat, přizpůsobovat požadavkům Objednatele a udržovat; nebo

b) pokud k takovému software není poskytnutí Licence v rozsahu dle čl. 15.3 Smlouvy účelné (zejména vývojový software, databázový software, kancelářský software, operační systém aj.).

Dodavatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

15.4.2 Jedná se o software, který je veřejnosti poskytován zdarma, včetně detailně komentovaných zdrojových kódů, úplné uživatelské, provozní a administrátorské dokumentace a práva software měnit. Dodavatel je povinen poskytnout Objednateli

o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

15.4.3 Jedná se o software, (i) který je integrální součástí hardware dodávaného jako část plnění Smlouvy, nebo (ii) který nad takovým hardware poskytuje pouze abstrakční vrstvu pro správu, konfiguraci, informační bezpečnost, programování aplikací nebo jiné obdobné účely, vše za podmínky, že spouštění takového software je od výrobce příslušného hardware předepsáno pro jeho korektní fungování a zároveň se jedná o software, k němuž není poskytnutí Licence v rozsahu dle čl. 15.3 Smlouvy účelné. Dodavatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

15.4.4 Dodavatel je povinen udržovat prohlášení dle tohoto čl. 15.4 Smlouvy v platnosti. V případě že Dodavatel poruší tuto povinnost, nepředloží Objednateli příslušné prohlášení či nejpozději do jednoho (1) měsíce na výzvu Objednatele relevantní skutečnosti neprokáže, je Objednatel oprávněn požadovat úhradu smluvní pokuty ve výši 100.000 Kč za každý jednotlivý případ a bezodkladné zajištění nápravy, a to včetně náhrady příslušného software.

15.4.5 Součástí Licence je též právo k provedeným změnám konfigurace či nastavením počítačových programů.

15.5 Pokud se bude jednat o standardní software dle čl. 15.4 Smlouvy, tak na rozdíl od Licence ke zbývajícím částem plnění udělované dle čl. 15.3 Smlouvy postačí, aby udělená Licence k takovému software zahrnovala nevýhradní oprávnění užít jej jakýmkoli způsobem nejméně po dobu dvou (2) let ode dne akceptace poslední dílčí části Díla, na území České republiky a v množstevním rozsahu, který je objektivně nezbytný pro pokrytí potřeb Objednatele ke dni uzavření této Smlouvy, a to včetně práva Objednatele do standardního software zasahovat, pokud tak stanoví příslušné ustanovení čl. 15.4 této Smlouvy.

15.6 Nelze-li to na Dodavateli spravedlivě požadovat a není-li to v rozporu s ustanoveními čl. 15.4 Smlouvy, nemusí být Objednateli ke standardnímu softwaru předány zdrojové kódy a stejně tak nemusí být Objednateli poskytnuto právo do standardního softwaru zasahovat, vždy však musí být předána kompletní uživatelská, administrátorská a provozní dokumentace. Součástí Licence je též právo k provedeným změnám konfigurace či nastavením počítačových programů.

15.7 Dodavatel se zavazuje samostatně zdokumentovat veškeré využití standardního software v rámci plnění a předložit Objednateli ucelený přehled využitého standardního software, jehož součástí budou licenční podmínky takového standardního software a seznam jeho alternativních dodavatelů. Tento přehled je Dodavatel povinen předložit Objednateli vždy do tří (3) pracovních dnů po akceptaci plnění, v jehož rámci Dodavatel využil standardní software a dále vždy do jednoho (1) měsíce od doručení výzvy Objednatele, kterou může Objednatel učinit kdykoli, nejpozději však do dvou (2) let od skončení platnosti Smlouvy z jakéhokoli důvodu.

15.8 Jestliže jsou s užitím standardního software spojeny jednorázové či pravidelné poplatky, je Dodavatel povinen v rámci Ceny Díla řádně uhradit všechny tyto poplatky nejméně po dobu dvou (2) let ode dne akceptace poslední dílčí Dodávky. Nad rámec Ceny Díla nebudou Dodavateli hrazeny žádné další poplatky či odměny.

15.9 Práva získaná v rámci plnění této Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Dodavatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Dodavatelem Objednateli.

15.10 Bez ohledu na formu uzavření licenční smlouvy platí, že Dodavatel je vždy povinen zajistit poskytnutí Licence dle podmínek stanovených Smlouvou, a to bez ohledu na případný rozdílný obsah standardních licenčních podmínek vykonavatele majetkových práv k takovým autorským dílům.

16. SMLUVNÍ POKUTY

16.1 **Smluvní pokuty.** Pokud jedna ze Smluvních stran (dále jen „**Porušující strana**“) poruší tuto Smlouvu nebo nesplní včas své povinnosti vyplývající z této Smlouvy, je Porušující strana povinna, kromě všech ostatních opravných prostředků, které má k dispozici podle této Smlouvy, nebo podle zákona a kterých se druhá Smluvní strana (dále jen „**Oprávněná strana**“) nezřekne uplatněním jakéhokoli práva podle tohoto čl. 16, zaplatit smluvní pokutu podle tohoto článku 16.

16.2 **Oddělitelnost**. Není-li v tomto čl. 16 uvedeno jinak, je Oprávněná strana oprávněna účtovat Porušující straně smluvní pokuty za každý jednotlivý případ jejího porušení této Smlouvy a/nebo jejího prodlení s plněním povinností.

16.3 **Prodlení s Plněním**. Smluvní strany se dohodly, že případě prodlení Dodavatele se splnění ve stanoveném Milníku dokončení dle Harmonogramu, které je způsobeno výhradně Dodavatelem, vzniká Objednateli nárok na zaplacení smluvní pokuty Dodavatelem ve výši 25.000 Kč za každý započatý den prodlení.

16.4 **Prodlení platby.** V případě prodlení Objednatele s úhradou Faktury má Dodavatel právo na úhradu úroku z prodlení v zákonné výši z dlužné částky včetně DPH za každý den, kdy je Objednatel v prodlení.

16.5 **Porušení povinností.** V případě porušení povinností Dodavatele uvedených v čl. 10.1.1 až 10.1.3 má Objednatel právo na úhradu smluvní pokuty ve výši 10.000 Kč za každé takové porušení.

16.6 **Neschválené změny poddodavatele. Neschválení změny člena realizačního týmu**. V případě, že Dodavatel bude k provádění díla využívat poddodavatele nebo členy realizačního týmu v rozporu s ustanoveními čl. 10.6 nebo čl. 10.7 této Smlouvy, vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 20.000 Kč za každý jednotlivý případ takového porušení Smlouvy.

16.7 **Bezpečnostní opatření.** V případě porušení povinností stanovených v čl. 20 ze strany Dodavatele má Objednatel právo na úhradu smluvní pokuty ve výši 50.000 Kč za každé takové porušení.

16.8 **Integrita dat.** V případě porušení integrity Dat Objednatele způsobeného výhradně Dodavatelem má Objednatel právo na úhradu smluvní pokuty ve výši 1.000.000 Kč za každé takové porušení.

16.9 **Ztráta dat.** V případě ztráty dat Objednatele způsobené výhradně Dodavatelem má Objednatel právo na úhradu smluvní pokuty ve výši 1.000.000 Kč za každé takové porušení.

16.10 **Zneužití dat.** V případě zneužití dat Objednatele způsobeného výhradně Dodavatelem, tj. v případě, že data Objednatele jsou z důvodů výhradně na straně Dodavatele využita Dodavatelem, Subdodavatelem nebo třetí osobou v rozporu s touto Smlouvou, má Objednatel právo na úhradu smluvní pokuty ve výši 10.000.000 Kč za každé takové porušení.

16.11 **Ochrana Důvěrných informací.** Poruší-li Dodavatel povinnosti vyplývající z této Smlouvy ohledně ochrany Důvěrných informací, je povinen zaplatit Objednateli smluvní pokutu ve výši 1.000.000 Kč za každé nikoliv nepodstatné porušení takové povinnosti.

17. NÁHRADA ÚJMY

17.1 Každá ze Smluvních stran nese odpovědnost za způsobenou újmu v rámci platných právních předpisů a této Smlouvy. Obě Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

17.2 Žádná ze Smluvních stran neodpovídá za újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany. V případě, že Objednatel poskytl Dodavateli chybné zadání a Dodavatel s ohledem na svou povinnost provádět Dílo s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.

17.3 Žádná ze Smluvních stran není odpovědná za újmu a není ani v prodlení, pokud k tomuto došlo výlučně v důsledku prodlení s plněním závazků druhé Smluvní strany nebo v důsledku překážek vylučujících povinnost k náhradě újmy ve smyslu § 2913 odst. 2 Občanském zákoníku (dále jen „**Vyšší moc**“).

17.4 Za Vyšší moc se podle této Smlouvy považují mimořádné nepředvídatelné a nepřekonatelné překážky bránící dočasně nebo trvale plnění povinností stanovených v této Smlouvě, pokud nastaly po jejím uzavření nezávisle na vůli povinné Smluvní strany a jestliže tyto překážky nemohly být povinnou Smluvní stranou odvráceny ani při vynaložení veškerého úsilí, které lze rozumně v dané situaci požadovat.

17.5 Za Vyšší moc se však nepokládají okolnosti, jež vyplývají z osobních nebo hospodářských poměrů povinné Smluvní strany a dále překážky plnění, které byla příslušná Smluvní strana povinna překonat nebo odstranit podle této Smlouvy, obchodních zvyklostí nebo obecně závazných právních předpisů nebo jestliže může důsledky své odpovědnosti smluvně převést na třetí osobu, jakož i okolnosti, které se projevily až v době, kdy povinná Smluvní strana již byla v prodlení.

17.6 Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé překážky vylučující povinnost k náhradě újmy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání překážek vylučujících povinnost k náhradě újmy. Každá ze Smluvních stran je oprávněna požadovat náhradu újmy v plném rozsahu i v případě, že se jedná o porušení povinnosti, na kterou se dle této Smlouvy vztahuje smluvní pokuta nebo sleva z ceny.

17.7 Případná náhrada újmy bude zaplacena v měně platné na území České republiky, přičemž pro propočet na tuto měnu je rozhodný kurs České národní banky ke dni vzniku újmy.

17.8 Každá ze Smluvních stran je oprávněna požadovat náhradu újmy i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta nebo sleva z ceny, a to v celém rozsahu nebo slevy z ceny dle této Smlouvy.

18. ZMĚNOVÉ ŘÍZENÍ, VYHRAZENÁ ZMĚNA ZÁVAZKU

18.1 Kterákoliv ze Smluvních stran je v průběhu trvání této Smlouvy oprávněna písemně navrhnout změny Technické specifikace. V případě, že změnu Technické specifikace navrhne Objednatel, je Dodavatel povinen vynaložit veškeré úsilí k tomu, aby změnu

Technické specifikace přijal. Objednatel není povinen přijmout změnu Technické specifikace navrhovanou Dodavatelem.

18.2 Dodavatel se na písemnou výzvu Objednatele zavazuje do deseti (10) pracovních dnů vyhodnotit důsledky navržených změn Technické specifikace, které budou zahrnovat hodnocení dopadů těchto změn na cenu a rozsah Díla, dohodnuté termíny Díla, rozsah potřebné součinnosti a jakékoliv další relevantní aspekty smluvního vztahu (dále jen „**Hodnocení důsledků**"). Pokud si vypracování Hodnocení důsledků vyžádá dodatečné náklady nebo pokud by jeho vypracování mohlo mít negativní dopad na plnění závazků Dodavatele dle této Smlouvy, vypracuje Dodavatel Hodnocení důsledků na základě písemné dohody s Objednatelem o úhradě nákladů na vypracování Hodnocení důsledků a o úpravě dalších smluvních podmínek, kterých se vypracování Hodnocení důsledků může dotknout.

18.3 Jakékoliv změny Technické specifikace či poskytování služeb dle Smlouvy musí být dohodnuty formou písemného dodatku k této Smlouvě podle čl. 23.1 Smlouvy, kterým dojde k úpravě smluvních podmínek v souladu s Hodnocením důsledků, není-li touto Smlouvou stanoveno jinak.

18.4 Jakékoliv změny Technické specifikace Smlouvy musí být sjednány v souladu s příslušnými právními předpisy včetně ZZVZ.

19. OCHRANA INFORMACÍ

19.1 Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy:

19.1.1 si mohou vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „**Důvěrné informace**"),

19.1.2 mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé Smluvní strany nebo i jejím opominutím přístup k Důvěrným informacím druhé Smluvní strany.

19.2 Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě Důvěrné informace, které při plnění této Smlouvy získala od druhé Smluvní strany.

19.3 Za třetí osoby podle čl. 19.2 Smlouvy se nepovažují:

19.3.1 zaměstnanci Smluvních stran a osoby v obdobném postavení,

19.3.2 orgány Smluvních stran a jejich členové,

19.3.3 ve vztahu k Důvěrným informacím Objednatele poddodavatelé Dodavatele,

19.3.4 ve vztahu k Důvěrným informacím Dodavatele externí Dodavatelé Objednatele, a to i potenciální,

za předpokladu, že se podílejí na plnění této Smlouvy nebo na plnění spojeném s Dílem dle této Smlouvy, Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění Důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny Smluvním stranám v této Smlouvě.

19.4 Smluvní strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit Důvěrné informace vyplývající z této Smlouvy a též z příslušných právních předpisů, zejména povinnosti vyplývající z nařízení Evropského parlamentu a Rady (EU) 2016/679 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), CELEX: 32016R0679 (dále jen „**Nařízení**“).

19.5 Smluvní strany pro vyloučení pochybností prohlašují, že při zpracování osobních údajů dle této Smlouvy vystupují jako samostatní správci dle Nařízení. V případě potřeb Smluvní strany uzavřou samostatnou Smlouvu o zpracování osobních údajů.

19.6 Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na plnění této Smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany Důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění této Smlouvy.

19.7 Budou-li údaje, ke kterým Dodavatel získá přístup v souvislosti s plněním dle této Smlouvy mít povahu osobních údajů dle Nařízení, je Dodavatel povinen přijmout veškerá opatření k tomu, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k těmto osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům či jinému zneužití, a zajistit nakládání s osobními údaji v souladu s Nařízením a příslušnými právními předpisy na ochranu osobních údajů.

19.8 Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající Smluvní strany a přijímající Smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní Důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, se obě Smluvní strany zavazují neduplikovat žádným způsobem Důvěrné informace druhé Smluvní strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Obě Smluvní strany se zároveň zavazují nepoužít Důvěrné informace druhé Smluvní strany jinak než za účelem plnění této Smlouvy.

19.9 Nedohodnou-li se Smluvní strany výslovně písemnou formou jinak, považují se za Důvěrné implicitně všechny informace, které jsou anebo by mohly být součástí obchodního tajemství, tj. například, ale nejenom, popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající Smluvní stranou by předávající straně mohlo způsobit újmu.

19.10 Bez ohledu na výše uvedená ustanovení se veškeré informace vztahující se k předmětu této Smlouvy a příslušné dokumentaci považují výlučně za Důvěrné informace Objednatele a Dodavatel je povinen tyto informace chránit v souladu s touto Smlouvou.

19.11 Pokud jsou Důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médiích), je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce nebo přední straně média. Absence takovéhoto upozornění však nezpůsobuje zánik povinnosti ochrany takto poskytnutých informací.

19.12 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

19.12.1 se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků přijímající Smluvní strany či právních předpisů,

19.12.2 mají být zpřístupněny Objednatelem na základě zákona, například zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších

předpisů, či jiného právního předpisu včetně práva EU nebo závazného rozhodnutí oprávněného orgánu veřejné moci, a Smluvní strany si v takovém případě poskytnou nezbytnou součinnost ke splnění takové zákonné povinnosti,

19.12.3 měla přijímající Smluvní strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi Smluvními stranami uzavřené Smlouvy o ochraně informací,

19.12.4 jsou výsledkem postupu, při kterém k nim přijímající Smluvní strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,

19.12.5 po podpisu této Smlouvy poskytne přijímající straně třetí osoba, jež není omezena v takovém nakládání s informacemi,

19.12.6 jsou obsažené ve Smlouvě a jsou uveřejněné dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) ve znění pozdějších předpisů (dále jen „**Zákon o registru smluv**“).

19.13 Za porušení povinnosti mlčenlivosti Smluvní stranou se považují též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v čl. 19.3 Smlouvy, které daná Smluvní strana poskytla Důvěrné informace druhé Smluvní strany.

19.14 Ukončení platnosti této Smlouvy z jakéhokoliv důvodu se nedotkne ustanovení tohoto čl. 19 Smlouvy a jejich účinnost přetrvá i po ukončení účinnosti této Smlouvy.

19.15 Dodavatel dále výslovně prohlašuje a bere na vědomí, že tato Smlouva nepředstavuje jeho obchodní tajemství ani neobsahuje jeho Důvěrné informace a souhlasí s tím, aby tato Smlouva byla v plném rozsahu zveřejněna v souladu se zákonnými povinnostmi Objednatele.

20. KYBERNETICKÁ BEZPEČNOST

20.1 Dodavatel prohlašuje, že je poskytovatelem regulované služby ve smyslu zákona č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

20.2 Dodavatel se zavazuje plnit a dodržovat veškeré povinnosti, které se na Dodavatele v této souvislosti vztahují.

20.3 Dodavatel prohlašuje, že má implementována veškerá bezpečnostní opatření k zajištění důvěrnosti, integrity a dostupnosti regulované služby v souladu se zákonem o kybernetické bezpečnosti a příslušnými prováděcími předpisy, a to minimálně v rozsahu požadavků uvedených v Příloze č. 6 této Smlouvy (dále jen „**Kybernetické požadavky**“).

20.4 Dodavatel umožní Objednateli v roční periodě po dobu trvání této Smlouvy a jeden (1) rok po ukončení trvání této Smlouvy provedení zákaznického auditu v souladu s požadavky Přílohy č. 6:

20.4.1 jehož rozsah bude ohraničen využíváním ICT prostředků Dodavatele pro potřeby plnění této Smlouvy a uloženými či zpracovávanými daty a informacemi Objednatele v ICT prostředí Dodavatele; a

20.4.2 jehož předmětem bude naplnění Kybernetických požadavků a hodnocení rizik dle Přílohy č. 6 této Smlouvy.

20.5 Objednatel je oprávněn při kontrole Kybernetických požadavků využít třetí stranu. V případě využití třetí strany bude Objednatel odpovídat za třetí stranu, jako by kontrolu prováděl sám, včetně odpovědnosti za způsobenou újmu.

20.6 Dodavatel umožní Objednateli kontrolu Kybernetických požadavků provedenou prostředky Objednatele nebo třetí strany, a to v lokalitě Dodavatele i vzdáleně, pokud to technické prostředky Dodavatele umožňují.

20.7 Dodavatel se zavazuje poskytnout Objednateli součinnost minimálně v rozsahu deset (10) ČD při provádění každého zákaznického auditu ze strany Objednatele a pro tuto činnost zajistit účast kvalifikovaných pracovníků.

20.8 Dále se Dodavatel zavazuje nedostatky zjištěné na základě provedeného hodnocení rizik dle Přílohy č. 6 této Smlouvy nebo v rámci provedeného auditu dle této Smlouvy a Přílohy č. 6 této Smlouvy odstranit ve lhůtě určené v písemném oznámení Objednatele. Nestanoví-li Objednatel lhůtu v písemném oznámení, zavazují se Smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší devadesát (90) dnů.

20.9 Dodavatel se dále dle této Smlouvy zavazuje:

20.9.1 poskytnout na vyžádání Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků;

20.9.2 na požádání s Objednatelem konzultovat kdykoli v průběhu provádění Díla dle této Smlouvy detailní nastavení bezpečnostních opatření k naplnění Kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků;

20.9.3 neprodleně informovat Objednatele o všech významných změnách v naplnění Kybernetických požadavků, které nastanou kdykoli v průběhu trvání této Smlouvy;

20.9.4 informovat Objednatele o významné změně ovládání Dodavatele. Ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích);

20.9.5 bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění Kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní;

20.9.6 bezodkladně informovat Objednatele o bezpečnostních incidentech, které mohou ovlivnit poskytování Služeb dle této Smlouvy; a

20.9.7 při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům a jejichž následkem může vzniknout újma nebo nesoulad se ZKB nebo jinými obecně závaznými právními předpisy.

20.10 Dodavatel se zavazuje dodávat pouze hardware, které splňuje požadavky právních předpisů na kybernetickou bezpečnost a digitální odolnost hardware jakožto věci s digitálním obsahem a digitálními prvky tak, aby je Dodavatel mohl bez omezení provozovat na území EHP.

21. DOBA TRVÁNÍ SMLOUVY A UKONČENÍ SMLOUVY

21.1 Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění v Zákoně o registru smluv dle a uzavírá se na dobu dvou (2) let od okamžiku akceptace poslední části Díla.

21.2 Tuto Smlouvu lze ukončit písemnou dohodou Smluvních stran.

21.3 Každá Smluvní strana je oprávněna odstoupit od této Smlouvy z důvodů stanovených touto Smlouvou.

21.4 Objednatel je oprávněn odstoupit od této Smlouvy v případě, že:

21.4.1 Dodavatel je v prodlení s plněním svých povinností déle než patnáct (15) kalendářních dní a nezjedná nápravu ani do deseti (10) kalendářních dnů ode dne doručení písemného oznámení Objednatele o takovém prodlení; nebo

21.4.2 dojde k porušení povinnosti ochrany Důvěrných informací dle této Smlouvy ze strany Dodavatele; nebo

21.4.3 na majetek Dodavatele je prohlášen úpadek, Dodavatel sám podá dlužnický návrh na zahájení insolvenčního řízení nebo insolvenční návrh je zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení (ve znění insolvenčního zákona); nebo

21.4.4 Dodavatel vstoupí do likvidace; nebo

21.4.5 Dodavatel předem neoznámí Objednateli jakoukoliv změnu osoby poddodavatele nebo zvětšení rozsahu plnění svěřeného poddodavateli ve smyslu čl. 10.6 této Smlouvy, nebo k takovéto změně Objednatel nedá předem souhlas dle téhož článku.

21.5 Dodavatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než šedesát (60) kalendářních dnů, pokud Objednatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Dodavatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než patnáct (15) kalendářních dnů od doručení takovéto výzvy.

21.6 Účinky odstoupení od Smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé Smluvní straně.

21.7 Objednatel je oprávněn tuto Smlouvu písemně vypovědět (a to i částečně) bez udání důvodů, a to s jedno (1) měsíční výpovědní dobou, která uplyne ke konci měsíce následujícího po měsíci doručení písemné výpovědi Dodavateli. Tuto výpověď nebo částečnou výpověď je Objednatel oprávněn učinit kdykoliv po dobu trvání této Smlouvy.

21.8 Ukončením platnosti této Smlouvy nejsou dotčena ustanovení Smlouvy týkající se Licencí, záruk, práv z vady, povinnosti nahradit újmu a povinnosti hradit smluvní pokuty, ustanovení o ochraně informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku platnosti této Smlouvy.

21.9 Zánikem platnosti této Smlouvy není dotčeno vzájemné plnění, pokud bylo řádně poskytnuto ani práva a nároky z takových plnění vyplývající. V případě, kdy by však Objednatel odstoupil od Smlouvy z důvodu takového porušení smluvní povinnosti Dodavatele, že se plnění Dodavatele stalo pro Objednatele nepotřebným, bude toto plnění Dodavateli vráceno a ten bude povinen vrátit Objednateli zaplacenou cenu.

22. ŘEŠENÍ SPORŮ

22.1 Práva a povinnosti Smluvních stran touto Smlouvou výslovně neupravené se řídí zákonem č. 89/20212 Sb., občanský zákoník, ve znění pozdějších předpisů a příslušnými právními předpisy souvisejícími.

22.2 Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této Smlouvy nebo v souvislosti s touto Smlouvou, včetně sporů o její výklad či platnost a usilovat o jejich vyřešení nejprve smírně prostřednictvím jednání oprávněných osob nebo pověřených zástupců, a to do šedesáti (60) kalendářních dnů ode dne doručení výzvy ke smírnému vyřešení sporu zaslané kteroukoliv Smluvní stranou druhé Smluvní straně.

22.3 Nebude-li sporná záležitost vyřešena dle čl. 22.2 této Smlouvy do šedesáti (60) kalendářních dnů ode dne doručení výzvy ke smírnému vyřešení sporu zaslané kteroukoliv Smluvní stranou druhé Smluvní straně, bude tento spor rozhodován s konečnou platností u příslušného obecného soudu České republiky. Smluvní strany se dohodly, že místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.

23. ZÁVĚREČNÁ USTANOVENÍ

23.1 **Změny a úpravy.** Tuto Smlouvu lze upravovat pouze dohodou Smluvních stran písemnými v řadě číslovanými dodatky s výjimkou

23.2 Uzavření smlouvy bylo odsouhlaseno usnesením Rady městské části č. 554/RMČ/2025 ze dne 16.9.2025.

23.3 **Vyhotovení.** Tato Smlouva je vyhotovena v elektronickém originále a podepsána uznávanými elektronickými podpisy.

23.4 **Uveřejnění v registru smluv.** Smluvní strany souhlasí s uveřejněním plného znění této Smlouvy v registru smluv podle Zákon o registru smluv a rovněž na profilu Objednatele, případně i na dalších místech, kde tak stanoví právní předpis. Uveřejnění Smlouvy prostřednictvím registru smluv zajistí Objednatel.

23.5 **Úplná dohoda.** Tato Smlouva spolu se všemi přílohami a jakýmikoliv dalšími dokumenty, které jsou do ní začleněny odkazem, představuje jedinou a úplnou dohodu Smluvních stran ohledně předmětu, který je v ní obsažen, a nahrazuje veškerá předchozí a současná ujednání a dohody, písemné i ústní, týkající se tohoto předmětu.

23.6 **Přílohy.** Nedílnou součástí této Smlouvy jsou následující přílohy:

1. Příloha č. 1 – Technická specifikace
2. Příloha č. 2 – Harmonogram
3. Příloha č. 3 – Součinnost Objednatele
4. Příloha č. 4 – Seznam poddodavatelů a členů realizačního týmu
5. Příloha č. 5 – Oprávněné osoby
6. Příloha č. 6 – Kybernetická bezpečnost
7. Příloha č. 7 – Ceník
8. Příloha č. 8 – Vzor Akceptačního protokolu

[*PODPISOVÁ STRANA NÁSLEDUJE*]

Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

PŘÍLOHA Č. 1 – TECHNICKÁ SPECIFIKACE

(Samostatná volná příloha Smlouvy)

PŘÍLOHA Č. 2 – HARMONOGRAM

Smluvní strany se dohodly, že realizace Díla bude rozdělena do dvou Projektových etap. K jednotlivým etapám se váže vždy odpovídající část Ceny Díla, která bude splatná na základě řádně vystavené Faktury po akceptaci příslušné etapy.

1. PROJEKTOVÁ ETAPA Č.1

1.1 Implementace a zprovoznění bezpečnostních funkcí v testovacím prostředí, včetně provedení Akceptačních testů a předání k akceptaci Objednateli.

1.2 Milník dokončení této Projektové etapy je stanoven do 30 dnů ode dne nabytí účinnosti Smlouvy.

1.3 Po řádné akceptaci této Projektové etapy vzniká Dodavateli nárok na úhradu první části Ceny Díla ve výši 1 361 600,00 Kč bez DPH.

2. PROJEKTOVÁ ETAPA Č.2

2.1 Implementace a zprovoznění bezpečnostních funkcí v produkčním prostředí, včetně provedení Akceptačních testů a předání k akceptaci Objednateli.

2.2 Milník dokončení této etapy je stanoven do 30 dnů ode akceptace Projektové etapy č. 1.

2.3 Po řádné akceptaci této Projektové etapy vzniká Dodavateli nárok na úhradu první části Ceny Díla ve výši 888 000,00 Kč bez DPH.

PŘÍLOHA Č. 3 – SOUČINNOST OBJEDNATELE

Pro řádné provedení Díla a jeho částí je nezbytná dobře fungující součinnost ze strany Objednatele, na základě které zejména:

1. Objednatel poskytne na svůj náklad podporu Dodavateli při realizaci Díla, zejména plynulé předávání potřebných informací.
2. Objednatel poskytne relevantní informace k realizaci Díla, vyžádané Dodavatelem, o současných postupech, procesech a organizačních opatřeních Objednatele potřebných pro realizaci Díla. Objednatel se zavazuje poskytovat Dodavateli úplné, pravdivé a včasné informace potřebné k řádnému průběhu realizace Díla a zavazuje se předávat Dodavateli potřebné podklady dohodnuté příslušnými orgány řízení realizace Díla, a to v dohodnutých Milnících.
3. Objednatel je povinen plnit řádně a včas úkoly, které pro něj vyplynou z jednání orgánů řízení realizace Díla. Úkolem se pro účely této Smlouvy rozumí provedení nějaké činnosti nebo poskytnutí informace, kdy tento úkol bude vždy podrobněji specifikován v protokolu o jednání orgánů řízení realizace Díla spolu se stanovením rozsahu úkolu, se závazným termín splnění úkolu a zodpovědnou osobou.
4. Pokud bude poskytování služeb prováděno v sídle Objednatele, zajistí Objednatel na svůj náklad veškeré potřebné předpoklady pro řádné poskytování služeb Dodavatelem, a to zejména pracovní místo, jehož součástí bude požadovaný počet projektových pracovišť pro práci aplikačních týmů, s přípojnými místy do sítě (případně wifi/VPN) a s přístupem k tiskárně.
5. Objednatel jmenuje z řad svých pracovníků dostatečný počet odborníků (pracovníků s odpovídající kvalifikací a zkušenostmi) do projektových týmů, dle potřeb je bude uvolňovat pro práci projektových týmů a zajistí dostatečné pravomoci vedoucímu realizace Díla ze strany Objednatele. Objednatel zajistí potřebné složení týmů v průběhu celé realizace Díla.
6. Pokud bude součástí provedení Díla podle této Smlouvy také realizace vazeb na aplikace třetí strany nebo realizace vazeb na jiný informační systém, jehož dodávka není součástí provedení Díla podle této Smlouvy, zajistí Objednatel na své náklady se subdodavateli těchto systémů koordinaci potřebnou pro splnění dotyčné části plnění.
7. Objednatel umožní Dodavateli a jeho pracovníkům plný přístup k vlastnímu programovému vybavení a k automatizovanému i neautomatizovanému informačnímu systému v rozsahu nezbytném pro řádný průběh realizace Díla a pro plnění uzavřených smluv.

PŘÍLOHA Č. 4 – SEZNAM PODDODAVATELŮ A ČLENŮ REALIZAČNÍHO TÝMU

Firma poddodavatele: Next Generation Security Solutions s.r.o.

Sídlo: U Uranie 954/18, Holešovice, 170 00 Praha 7

Právní forma: 112 – Společnost s ručením omezeným

Identifikační číslo: 06291031

Rozsah plnění Smlouvy: 30 %, Konzultační činnost, Podpora dosažení akceptačních kritérií, Metodická podpora, Konzultace a dohled

Seznam členů realizačního týmu

Pozice (role)	Identifikační údaje osoby	Dodavatel/ člen společnosti dodavatelů / poddodavatel, k němuž osoba patří
Vedoucí zakázky	[redacted]	

PŘÍLOHA Č. 5 – OPRÁVNĚNÉ OSOBY

Oprávněná osoba **za Objednatele** ve věcech smluvních:

Jméno a příjmení	[redacted]
Pozice	
E-mail	
Telefon	

Oprávněná osoba **za Objednatele** ve věcech technických:

Jméno a příjmení	[redacted]
Pozice	
E-mail	
Telefon	

Oprávněná osoba za **Dodavatele** ve věcech smluvních

Jméno a příjmení	Tomáš Pokluda
Pozice	KeyAccount Manager
E-mail	tomas.pokluda@aricoma.com
Telefon	+420 775 851 742

Oprávněná osoba za **Dodavatele** ve věcech technických

Jméno a příjmení	Marcel Vojtíšek
Pozice	Projektový manažer
E-mail	marcel.vojtisek@aricoma.com
Telefon	+420 606 709 000

PŘÍLOHA Č. 6 – KYBERNETICKÁ BEZPEČNOST

Za účelem povinností stanovených Objednateli jakožto poskytovali regulované služby v oblasti řízení bezpečnosti dodavatelského řetězce, je Dodavatel povinen nad rámec povinností stanovených Smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této Přílohy č. 6 této Smlouvy.

Dodavatel je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy bezpečnostních opatření, kybernetických bezpečnostních incidentů, protiopatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje Objednateli, jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je Objednatel oprávněn požadovat od Dodavatele přiměřenou součinnost i nad rámec povinností stanovených v této Příloze č. 6 této Smlouvy, avšak vždy pouze za účelem zajištění plnění povinnosti Dodavatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

1. OBECNÁ USTANOVENÍ

1.1 Tato příloha (dále jen „**Příloha**“) tvoří nedílnou součást Smlouvy. Povinnosti Dodavatele uvedené v této příloze se vztahují výhradně ke Službám, které jsou předmětem Smlouvy.

1.2 Není-li dále stanoveno jinak nebo nevyplývá-li jinak z kontextu, mají pojmy počínající velkým písmenem v této Příloze shodný význam, jaký mají ve Smlouvě. Smluvní strany nad rámec Smlouvy vymezují následující pojmy:

1.2.1 **Data** znamenají data, záznamy, soubory, obsah, osobní údaje a další informace Objednatele, (a) shromážděné, přijaté nebo uchovávané Dodavatelem v souvislosti s plněním Smlouvy; (b) poskytnuté Objednatelem; nebo (c) odvozené z (a) a (b). Data podle této Smlouvy jsou klasifikována jako důvěrné informace, nebo se z jiných důvodů jedná o údaje vyžadující ochranu před neoprávněným přístupem, únikem, porušením nebo jiným odhalením;

1.2.2 **ZKB** znamená zákon č. 264/2025 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

1.3 Rozsah zapojení Dodavatele na rozvoji a provozu primárních a podpůrných aktiv Objednatele je určen předmětem Smlouvy a jejími přílohami včetně této Přílohy. Rozsah zapojení Dodavatele na zajištění bezpečnosti těchto aktiv je určen zejména touto Přílohou.

2. BEZPEČNOST INFORMACÍ

2.1 Dodavatel se zavazuje při nakládání s Daty chránit jejich důvěrnost, dostupnost a integritu s ohledem na jejich povahu a klasifikaci v souladu s touto Přílohou a dále v souladu se standardním bezpečnostním rámcem ISO 27001, případně dalším bezpečnostním rámcem jako např. NIST Cyber Security Framework nebo SSAE 18 SOC 2, a to do té míry, do jaké to není v rozporu s touto Přílohou.

2.2 Dodavatel je povinen zavést vhodná bezpečnostní opatření pro ochranu Dat alespoň v rozsahu této Přílohy.

2.3 Dodavatel jmenuje odpovědnou kontaktní osobu ve věcech kybernetické bezpečnosti pro potřeby zajištění plnění požadavků podle této Přílohy a Smlouvy v oblasti kybernetické bezpečnosti a související komunikace s Objednatelem. Poskytovatel je povinen oznámit kontaktní údaje této osoby Objednateli v **Příloze č. 3** Smlouvy – „Oprávněné osoby".

3. UŽITÍ A ZPŘÍSTUPNĚNÍ DAT

3.1 Dodavatel je oprávněn používat nebo sdílet Data pouze pro účely a způsobem, který stanoví Smlouva a její přílohy, a v souladu s příslušnými právními předpisy, po dobu trvání Smlouvy a po jejím ukončení, dokud má Dodavatel Data nadále ve své dispozici.

3.2 Dodavatel bere na vědomí, že veškerá Data zůstávají předmětem výhradních práv Objednatele, který je jediným vlastníkem Dat a pořizovatelem databází, ve kterých jsou Data uložena.

3.3 Dodavatel se zavazuje zachovávat mlčenlivost o Datech a jejich obsahu.

3.4 Dodavatel se zavazuje šifrovat v prostředí Poskytovatele uložená Data minimálně v souladu se standardem šifrování dat AES-256.

3.5 Dodavatel je povinen omezit přístup k Datům Objednatele pouze na ty zaměstnance a třetí strany, u kterých přístup vyžaduje plnění Smlouvy nebo plnění zákonných povinností. Dodavatel nesmí umožnit přístup k Datům Objednatele jiným třetím stranám bez předchozího písemného souhlasu Objednatele. Vysloví-li Objednatel v souladu se Smlouvou nebo jinak písemně souhlas se zapojením konkrétního poddodavatele do plnění Smlouvy, uděluje tím souhlas se zpřístupněním Dat Objednatele poddodavateli v rozsahu nezbytném pro plnění Smlouvy poddodavatelem.

3.6 V případě, že Objednatel při hodnocení rizik spojených se Smlouvou identifikuje skutečnosti, jejichž existence tvoří:

3.6.1 kybernetickou hrozbu a výskyt této hrozby je velmi pravděpodobný až víceméně jistý či předpokládaná realizace hrozby je častější než jednou za měsíc, nebo

3.6.2 riziko pro předmět Smlouvy a toto riziko je na natolik závažné (kritické), že jeho existence je nepřípustná a musí být neprodleně zahájeny kroky k jeho odstranění,

3.6.3 může Objednatel Dodavateli uložit přijetí dalších bezpečnostních opatření ve smyslu ZKB, případně zákona, který ZKB nahradí. Objednatel při naplnění podmínek výše předá Dodavateli popis vybraných bezpečnostních opatření, která navrhuje zavést ke snížení identifikovaného rizika. Dodavatel je oprávněn bez zbytečného odkladu, nejpozději však do 15 pracovních dní, podat připomínky k formě zvolených bezpečnostních opatření (včetně přehledu očekávaných finančních dopadů na zavedení bezpečnostních opatřeních na straně Dodavatele) a případně navrhnout jinou formu zvolených bezpečnostních opatření. Dohodnou-li se Objednatel

a Dodavatel na zavedení bezpečnostních opatření, na termínu jejich zavedení a na tom, kdo ponese náklady na jejich zavedení, je Dodavatel povinen bez zbytečného odkladu zavést daná bezpečnostní opatření a jejich zavedení oznámit Objednateli.

3.7 V případě, že cizozemský orgán požádá o zpřístupnění nebo předání Dat zpracovávaných na území cizího státu, Objednatel takové žádosti vyhoví:

3.7.1 až po provedení přezkoumání zákonnosti žádosti,

3.7.2 až po vynaložení veškerého úsilí k zabránění zpřístupnění nebo předání Dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování Dat nebo podle kterého byla žádost podána,

3.7.3 pouze v nezbytném rozsahu.

4. AUTORSTVÍ PROGRAMOVÉHO KÓDU A LICENCE

4.1 Smluvní strany ve Smlouvě sjednaly právo Objednatele k předmětům duševního vlastnictví. Úprava práv Objednatele k předmětům duševního vlastnictví se řídí Smlouvou.

5. BEZPEČNOSTNÍ DOKUMENTACE

5.1 Dodavatel se v souvislosti s řízením kybernetické bezpečnosti zavazuje vypracovat a udržovat příslušnou bezpečnostní dokumentaci týkající se nastaveného systému řízení bezpečnosti informací a zabezpečení plnění Smlouvy, minimálně v rozsahu dle této Přílohy.

5.2 Dodavatel je povinen bezpečnostní dokumentaci podle této Přílohy pravidelně revidovat a aktualizovat, nejméně však 1× za rok, a kdykoli při významné změně a materiální změně skutečností zachycených v bezpečnostní dokumentaci.

6. ŘÍZENÍ AKTIV

6.1 Dodavatel se zavazuje minimálně:

6.1.1 identifikovat primární a podpůrná aktiva využívaná pro plnění Smlouvy;

6.1.2 určit vazby mezi primárními a podpůrnými aktivy a případně určit vazby na současná aktiva Objednatele;

6.1.3 tento seznam aktiv a jejich vazby udržovat aktuální a na vyžádání ho zpřístupnit (ve formě nahlédnutí) Objednateli.

7. ŘÍZENÍ RIZIK

7.1 Dodavatel se zavazuje minimálně:

7.1.1 řídit rizika, která mohou ovlivnit poskytování předmětu plnění Smlouvy, v souladu s následujícími minimálními požadavky na řízení rizik:

a) stanovit metodiku pro určování a hodnocení rizik, včetně kritérií pro akceptovatelnost rizik,

b) při určování rizik s ohledem na aktiva určit relevantní hrozby a zranitelnosti,

c) provádět hodnocení rizik v pravidelných intervalech alespoň jednou ročně a při významných změnách, přičemž budou zohledněny relevantní hrozby a zranitelnosti a posouzeny možné dopady na aktiva využívaná pro plnění Smlouvy,

d) zpracovat přehled všech bezpečnostních opatření, která byla aplikována, včetně způsobu plnění,

e) zpracovat plán zvládání rizik, který obsahuje minimálně popis bezpečnostních opatření a konkrétní způsob jejich realizace, cíle a přínosy bezpečnostních opatření a určení odpovědností,

f) zavádět bezpečnostní opatření v souladu s plánem zvládání rizik;

7.1.2 informovat Objednatele o způsobu řízení rizik, zbytkových rizicích souvisejících s plněním Smlouvy a předložit Objednateli zprávu o hodnocení aktiv a rizik, která jsou využívána pro plnění Smlouvy a o zbytkových rizicích souvisejících s aktivy využívanými pro plnění Smlouvy do 30 dnů od data účinnosti Smlouvy a následně v intervalu jednou za dva roky nebo v případě významné změny ovlivňující bezpečnost těchto aktiv;

7.1.3 reagovat na změny a upravit na své straně bezpečnostní opatření tak, aby odpovídala novému stavu po provedení změny;

7.1.4 pravidelně (minimálně 1× ročně) testovat zranitelnosti poskytovaných Služeb, a to prostřednictvím pravidelného penetračního testování a kontroly nasazených aktualizací, aby bylo zajištěno, že jsou bezpečnostní opatření aktuální vůči novým hrozbám. Poskytovatel je povinen o výsledcích testování dle tohoto odstavce Objednatele písemně informovat neprodleně po vyhotovení závěrečné zprávy z takového testování.

8. BEZPEČNOST LIDSKÝCH ZDROJŮ

8.1 Poskytovatel se zavazuje minimálně:

8.1.1 prověřit každého pracovníka před umožněním přístupu k aktivům Objednatele nebo před jeho zapojením do činností, které by mohly ovlivnit předmět plnění Smlouvy, a to alespoň z hlediska:

a) kontroly dosaženého vzdělání a odborné kvalifikace,

b) profesních zkušeností, jde-li o pracovníky, kteří mají zastávat bezpečnostní nebo administrátorské role;

8.1.2 zavést pravidelné školení svých pracovníků v oblasti kybernetické bezpečnosti a základní kybernetické hygieny a vést o tomto školení spolehlivou evidenci;

8.1.3 poučit své pracovníky o požadavcích dle této Přílohy před umožněním jejich přístupu k Datům nebo před jejich zapojením do činností, které by mohly ovlivnit bezpečnost v souvislosti s předmětem plnění Smlouvy;

8.1.4 zajistit, aby pracovníci před umožněním jejich přístupu k Datům nebo před zapojením do činností, které by mohly ovlivnit bezpečnost předmětu plnění Smlouvy, měli uzavřenou dohodu o zachování mlčenlivosti (důvěrnosti) Dat s adekvátní dobou trvání povinnosti mlčenlivosti;

8.1.5 zajistit procesy a pravidla vedení disciplinárního řízení (zejména odstupňované reakce) a v případě potřeby provádět disciplinární řízení k přijetí opatření vůči pracovníkům, kteří porušili povinnosti v oblasti kybernetické bezpečnosti;

8.1.6 zajistit dostatečnou míru zastupitelnosti pro technické bezpečnostní aspekty plnění Smlouvy.

8.2 Poddodavatel Dodavatele, který přistupuje k Datům, je povinen dodržovat veškeré povinnosti uvedené v čl. 8.1 této Přílohy ve vztahu ke svým zaměstnancům, případně dalším osobám, které se podílejí na realizaci předmětu plnění Smlouvy dle pokynů poddodavatele Dodavatele. Dodavatel je povinen poddodavatele o povinnostech plynoucích z čl. 8.1 této Přílohy řádně poučit a uzavřít s poddodavatelem písemnou smlouvu v souladu s čl. 23 této Přílohy.

9. ŘÍZENÍ PROVOZU

9.1 Dodavatel se zavazuje minimálně:

9.1.1 stanovit práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role;

9.1.2 stanovit pravidla a postupy pro ochranu před škodlivým kódem;

9.1.3 stanovit pravidla a postupy pro řízení technických zranitelností;

9.1.4 stanovit pravidla a postupy k provádění pravidelného zálohování a kontroly použitelnosti prováděných záloh;

9.1.5 stanovit pravidla pro zajištění oddělení vývojového, testovacího a provozního prostředí.

10. ŘÍZENÍ ZMĚN

10.1 Dodavatel se zavazuje minimálně:

10.1.1 sledovat a identifikovat změny, které mají nebo mohou mít vliv na zajištění kybernetické bezpečnosti Dat a informovat Objednatele o této skutečnosti;

10.1.2 poskytnout Objednateli veškeré potřebné informace a součinnost v procesu řízení a evidence změn. Informace musí být poskytnuty v rozsahu, který Objednateli umožní:

a) posoudit, zda změna ve vztahu k plnění dle Smlouvy je významnou změnou,

b) posoudit rizika související s významnou změnou ve vztahu k plnění dle Smlouvy, testovat změnu před nasazením do provozu a posoudit možnost případného navrácení do původního stavu,

c) přijmout přiměřená opatření ke zvládání rizik souvisejících s touto změnou, nebo změnu vůbec neprovést, pokud nelze přijmout opatření snižující tato rizika na akceptovatelnou úroveň,

d) dokumentovat posouzení rizik souvisejících s významnou změnou ve vztahu k plnění dle Smlouvy a přijatá opatření, a

e) provést další činnosti u významných změn dle potřeb Objednatele;

10.1.3 reagovat na významné změny, zejména aktualizovat hodnocení rizik, bezpečnostní a provozní dokumentaci a upravit na své straně bezpečnostní opatření tak, aby odpovídala novému stavu po provedení změny.

11. ŘÍZENÍ KONTINUITY ČINNOSTÍ

11.1 Dodavatel se v rozsahu předmětu plnění dle Smlouvy zavazuje zavést a udržovat vhodná opatření pro zajištění kontinuity činností. Zejména se Dodavatel zavazuje:

11.1.1 zajistit adekvátní kontinuitu aktiv, která jsou potřebná k poskytování plnění dle Smlouvy; a

11.1.2 pravidelně kontrolovat a testovat, že je schopen zajistit kontinuitu aktiv při dodržení sjednané úrovně plnění dle Smlouvy.

11.2 Dodavatel se zavazuje poskytnout nezbytnou součinnost při zpracování a testování plánů kontinuity, plánů obnovy a havarijních plánů a plnění dalších povinností Objednatele a následně v případě aktivace plánů kontinuity, plánů obnovy nebo havarijních plánů, poskytnout nezbytnou součinnost při jejich plnění. Objednatel se zavazuje uhradit Dodavateli účelně vynaložené náklady na poskytnutí této součinnosti.

12. AKVIZICE, VÝVOJ A ÚDRŽBA

12.1 Dodavatel se zavazuje minimálně:

12.1.1 zajistit, aby zajištění bezpečnosti informací bylo zahrnuto do všech vývojových, implementačních či akvizičních projektů, kde je reálné narušení informační bezpečnosti Dat a ochrany soukromí, a vyčlenit pro tento účel potřebné zdroje;

12.1.2 zajistit oddělení vývojového, testovacího a provozního prostředí;

12.1.3 dodržovat nejlepší praxi v oblasti bezpečného vývoje a postupovat při vývoji v souladu s dalšími pokyny Objednatele.

13. ŘÍZENÍ PŘÍSTUPU

13.1 Dodavatel se zavazuje minimálně:

13.1.1 provozovat ke zpracování Dat pouze taková aktiva, která umožňují správu rolí a uživatelů a která neumožní činnost uživatelů bez autentizace a zároveň umožňují ochranu autentizačního mechanismu před neoprávněným přístupem a prolomením autentizačních parametrů;

13.1.2 zajistit, aby uživatelské účty byly adekvátně chráněny prostřednictvím autentizačních mechanismů;

13.1.3 zajistit, aby uživatelé chránili své uživatelské účty, zejména své autentizační údaje a nástroje a aby neposkytli tyto údaje třetí straně;

13.1.4 udělovat přístup pracovníkům podle zásady „need-to-know“ a průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu;

13.1.5 zajistit kontrolu podezřelých přístupů a aktivit;

13.1.6 v případě potřeby bezodkladně odebrat přístupová oprávnění, zejména pokud

a) zaměstnanec již nepotřebuje přístup k plnění svých pracovních povinností (např. pokud došlo ke změně pozice zaměstnance/odchod z projektu apod.),

b) zaměstnanec se dopustil závažného porušení povinností v oblasti kybernetické bezpečnosti nebo existují důvodné obavy, že se takového porušení dopustí,

c) zaměstnanec nesplňuje požadavky na přístup k Datům nebo požadavky na zapojení do činností, které by mohly ovlivnit bezpečnost předmětu plnění Smlouvy,

d) se ukáže potřeba přijmout mimořádné bezpečností opatření spočívající v odebrání přístupu (zejména pokud Poskytovatel dal zaměstnanci výpověď z výpovědního důvodu podle § 52 písm. f), g) a h) zákoníku práce),

e) byl ukončen pracovní poměr (nebyl-li přístup odebrán dříve),

f) došlo k úniku autentizačních údajů (hesla);

13.1.7 vést evidenci o udělených a odebraných přístupových oprávněních;

13.1.8 vést evidenci o všech přístupech k Datům Objednatele, kdy je Dodavatel povinen archivovat záznamy o všech přístupech po dobu 1 roku;

13.1.9 zajistit zabezpečení a správu koncových zařízení (pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA apod.) prostřednictvím kterých lze přistupovat k Datům, a to minimálně v rozsahu seznámení uživatelů a zajištění souladu s politikou pro šifrování Dodavatele.

14. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

14.1 Dodavatel se zavazuje minimálně:

14.1.1 zajistit, aby jeho pracovníci a poddodavatelé oznamovali neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti a hrozby;

14.1.2 po dobu 6 měsíců vést a uchovávat záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání;

14.1.3 prošetřit a určit příčiny kybernetického bezpečnostního incidentu;

14.1.4 poskytnout Objednateli aktivní součinnost a relevantní informace o příčinách, podezřelém zařízení či osobě na straně Dodavatele v případě kybernetického bezpečnostního incidentu souvisejícího s Daty;

14.1.5 navrhnout a realizovat Dodavatelem odsouhlasená bezpečnostní opatření dle požadavků Objednatele v dohodnutých termínech pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu nebo hrozby;

14.1.6 vypracovat plán reakce na incidenty, který bude obsahovat konkrétní plán kroků, které musí Dodavatel případně i Objednatel, dodržet v případě bezpečnostního incidentu, a to ve vztahu k jednotlivým potenciálním druhům incidentů, a postupovat v souladu s tímto plánem.

15. FYZICKÁ BEZPEČNOST

15.1 Dodavatel se zavazuje minimálně:

15.1.1 zajistit dodržování politiky čistého stolu;

15.1.2 zajistit kanceláře, pracovní místnosti a prostory v případě jejich opuštění tak, aby nemohlo dojít k nedovolenému vstupu neoprávněných osob;

15.1.3 zajistit uzamykání pracovních stolů, skříní, kontrolovat uzavření oken;

15.1.4 zajistit dodržování režimových opatřeních v případě režimových pracovišť (perimetr s řízeným vstupem).

16. BEZPEČNOST KOMUNIKAČNÍCH SÍTÍ

16.1 Dodavatel se zavazuje minimálně:

16.1.1 zajistit vhodnou segmentaci komunikační sítě;

16.1.2 zajistit, aby komunikační síť byla chráněna bezpečným rozhraním, přičemž bude povolena pouze nutná komunikace;

16.1.3 zajistit, aby na síťových zařízeních byly spuštěny pouze nutné služby;

16.1.4 zajistit, aby byly sledovány zranitelnosti nasazených síťových zařízení a aby zjištěné zranitelnosti byly odstraňovány v dostatečných intervalech;

16.1.5 zajistit, aby přenos informací a dat v rámci komunikační sítě byl šifrován.

17. SPRÁVA A OVĚŘOVÁNÍ IDENTIT

17.1 Dodavatel se zavazuje minimálně:

17.1.1 používat nástroj pro správu a ověření identity (autentizační mechanismus), který přenáší a ukládá autentizační parametry v šifrované podobě;

17.1.2 používat autentizační mechanismus, který je založený na více faktorové autentizaci s nejméně dvěma různými typy faktorů, pokud je to možné;

17.1.3 v případě ztráty, vyzrazení nebo podezření na kompromitaci autentizačních nástrojů nebo parametrů okamžitě změnit parametry autentizace;

17.1.4 aktiva, která nepodporují více faktorovou autentizaci, dočasně zajistit autentizací pomocí podobně silných kryptografických klíčů nebo hesel;

17.1.5 v rámci systému vynucovat hesla s vlastnostmi podle aktuální nejlepší praxe, pokud je autentizace založena na heslech a nevyužívá se více faktorové autentizace.

18. OCHRANA PŘED ŠKODLIVÝM KÓDEM

18.1 Dodavatel se zavazuje minimálně:

18.1.1 zajistit použití nástroje pro nepřetržitou automatickou ochranu koncových zařízení;

18.1.2 monitorovat a řídit používání výměnných zařízení a datových nosičů a řídit jejich automatické spouštění;

18.1.3 provádět pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.

19. DETEKCE, ZAZNAMENÁVÁNÍ A VYHODNOCOVÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

19.1 Dodavatel se zavazuje minimálně:

19.1.1 zajistit, aby všechny klíčové prvky propojující významné uzly interních komunikačních sítí, bezpečnostní síťové prvky a všechny prvky na vnějším perimetru měly aktivní monitorování kybernetických bezpečnostních událostí;

19.1.2 zajistit, aby monitorování sítě zajišťovalo ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi, ověření a kontrolu přenášených dat na perimetru komunikační sítě;

19.1.3 zajistit, aby detekovaná nežádoucí komunikace byla automaticky blokována;

19.1.4 zajistit, aby po dobu 6 měsíců byly zaznamenávány kybernetické bezpečnostní události narušující integritu síťových prvků nebo síťové komunikace, aby tyto záznamy byly uchovány a poskytnuty Objednateli na vyžádání;

19.1.5 zajistit, aby primární reakcí byla eskalace bezpečnostní události nebo incidentu do příslušných hlášení, případně přímá eskalace na příslušné odpovědné pracovníky.

20. APLIKAČNÍ BEZPEČNOST

20.1 Dodavatel se zavazuje minimálně:

20.1.1 užívat technická aktiva, která jsou podporována;

20.1.2 sledovat dostupnost opravných balíčků nebo záplat a zajistit bezodkladnou bezpečnostní aktualizaci;

20.1.3 pokud není bezpečnostní aktualizace dostupná, zajistit jiné kompenzační řešení, případně zranitelnost může být akceptována.

21. KRYPTOGRAFICKÉ ALGORITMY

21.1 Dodavatel se zavazuje minimálně:

21.1.1 používat pouze aktuálně doporučované a odolné kryptografické algoritmy a kryptografické klíče podle nejlepší praxe.

22. KONTROLA A AUDIT

22.1 Objednatel je oprávněn, na základě předchozí výzvy ze strany Objednatele doručené v přiměřeném časovém předstihu (nejméně však 30 dní předem), provést kontrolu a audit údajů, účtů, záznamů, pracovních postupů, dokumentace, aktiv, prostor (včetně kontroly fyzického perimetru) a technických prostředků vztahujících se k plnění Smlouvy a této Přílohy, a to za účelem ověření plnění povinností vyplývajících ze Smlouvy, jejích příloh a této Přílohy (dále jen „**Audit**“).

22.2 Audit bude prováděn dle potřeb Objednatele a pak mimořádně v případech bezpečnostních událostí, důvodného podezření na nedostatečnou úroveň ochrany aktiv Objednatele, důvodného podezření na nakládání s aktivy v rozporu s relevantními ustanoveními Smlouvy a důvodného podezření na nedodržení bezpečnostních opatření, podle této Přílohy.

22.3 Audit bude prováděn Objednatelem nebo jím pověřenou třetí stranou smluvně zavázanou k mlčenlivosti minimálně v rozsahu odpovídajícím povinnostem mlčenlivosti Objednatele dle Smlouvy, a která není k Dodavateli v soutěžním nebo jiném konkurenčním postavení.

22.4 Dodavatel poskytne veškerou nezbytnou součinnost k řádnému provedení a dokončení Auditu, zejména umožní přístup k údajům, účtům, záznamům, pracovním postupům, dokumentaci, jiným dokladům či podkladům, k aktivům, do prostor (včetně kontroly fyzického perimetru) a k technickým prostředkům vztahujícím se k plnění Smlouvy a této Přílohy za účelem uskutečnění Auditu. Dodavatel zajistí součinnost kvalifikovaných pracovníků.

22.5 Jakákoliv data, informace nebo jiná aktiva získaná při Auditu mohou být použita výhradně pro účely Auditu, vyhodnocení jeho výsledků a přijetí navazujících opatření, a další potřeby Objednatele při řízení vztahu s Dodavatelem.

22.6 Dodavatel je povinen bez zbytečného odkladu, nejpozději však do 1 měsíce od ukončení auditu, předložit Objednateli návrhy opatření napravujících nedostatky zjištěné při Auditu. Jednotlivá opatření navržená v návaznosti na výsledky Auditu podléhají před jejich přijetím Dodavatelem předchozímu schválení ze strany Objednatele. Návrhy zřejmě nevhodných či neúčinných opatření Objednatel odmítne a Dodavatel je povinen v přiměřené lhůtě stanovené Objednatelem navrhnout jiná vhodná opatření. Dodavatel je taktéž povinen se na výzvu Objednatele podrobit dodatečné kontrole ze strany Objednatele nebo osoby, která Audit provedla, za účelem ověření nápravy nedostatků zjištěných při Auditu a kontroly přijatých opatření.

23. PODDODAVATELÉ A JEJICH ŘETĚZENÍ

23.1 Dodavatel se zavazuje, že pravidla dle této Přílohy budou dodržovat i poddodavatelé Dodavatele a jejich pracovníci podílející se na plnění Smlouvy. Dodavatel

Objednateli na písemné vyžádání doloží, že u poddodavatelů smluvně vyžaduje dodržování pravidel dle této Přílohy, a to poskytnutím příslušné smlouvy s konkrétním poddodavatelem do 10 dnů ode dne jejího vyžádání Objednatelem (Dodavatel může anonymizovat části smlouvy, které považuje za obchodní tajemství do té míry, aby anonymizace nebránila Objednateli v kontrole plnění povinnosti dle tohoto článku).

23.2 Dodavatel se zavazuje soustavně (případně pravidelně dle povahy) dohlížet na plnění této Přílohy ze strany jeho poddodavatelů a jejich pracovníků, vyžadovat a vymáhat její plnění.

23.3 Za porušení pravidel dle této Přílohy poddodavatelem odpovídá Dodavatel Objednateli jako by je porušil sám. Dodavatel odpovídá za zajištění dostatečné znalosti pravidel dle této Přílohy ze strany poddodavatelů a jejich pracovníků.

23.4 Dodavatel je oprávněn využít k plnění dle Smlouvy poddodavatele za podmínek stanovených Smlouvou.

24. PŘEDÁNÍ A LIKVIDACE DAT

24.1 Dodavatel se zavazuje na základě výzvy Objednatele bez zbytečného odkladu předat Objednateli bezpečným způsobem, ve strojově čitelné podobě a ve formátu zaručujícím kompatibilitu v procesu migrace jakákoli Data v dispoziční sféře Dodavatele (pokud jde o data v databázích pak ve standardním exportním formátu dané databáze, aby bylo možné předaný soubor co nejjednodušším způsobem bez nutnosti dalších nedůvodných úprav nasadit do databáze na produkčním prostředí). Dodavatel se k výzvě Objednatele zavazuje poskytnout nezbytnou součinnost, přičemž si Smluvní strany mohou písemně dohodnout jiný způsob předání Dat. Dodavatel je povinen, i bez výzvy Objednatele, předat Objednateli Data do sedmi (7) dnů po skončení účinnosti Smlouvy.

24.2 Smluvní strany při ukončení Smlouvy z jakéhokoli důvodu vyvinou veškeré úsilí k tomu, aby do doby dokončení migrace Dat či převodu plnění dle Smlouvy k Objednateli nebo jinému dodavateli, nedošlo k narušení parametrů plnění ve Smlouvě do té doby definovaných, a aby případný nový dodavatel dostal veškeré informace o plnění Smlouvy potřebné pro pokračování nebo nahrazení takového plnění.

24.3 Dodavatel se zavazuje do 30 dnů od obdržení výzvy Objednatele předat Objednateli:

24.3.1 aktualizovanou dokumentaci, kterou vytvořil nebo spravuje,

24.3.2 úplný a aktuální zdrojový kód v případech, kde se Smlouvou zavázal k jeho předání,

24.3.3 seznam platných administrátorských účtů využívaných v prostředí Objednatele,

24.3.4 úplnou „knowledge base“ týkající se poskytování Služeb, vč. popisu a seznamu uzavřených a neuzavřených servisních požadavků,

24.3.5 aktuální seznam standardních provozních úkonů pro údržbu aktiv Objednatele, kterých se Smlouva týká.

24.4 Dodavatel se zavazuje při ukončení účinnosti Smlouvy, případně na písemnou žádost Objednatele, bez zbytečného odkladu po předání Dat, nejpozději však do 14 dnů, zlikvidovat Data v souladu s touto Přílohou za podpůrného užití pravidel v následující tabulce, to vše za možného dozoru zástupce Objednatele. Tato povinnost se nevztahuje na Data, která Dodavatel potřebuje za účelem plnění zákonné povinnosti či povinnosti stanovené mu rozhodnutím správního orgánu či za účelem hájení oprávněných zájmu Dodavatele (například v případě probíhajícího či hrozícího sporu).

24.5 Tabulka č. 1: Pravidla pro likvidaci dat

Přípustný způsob likvidace podle úrovně důležitosti aktiva		
Způsob likvidace	**Popis způsobu likvidace**	**Přípustnost využití způsobu likvidace dle úrovně důležitosti aktiva**
Odstranění	Způsob likvidace nosičů informací a Dat tak, aby byla nedostupná (například odstranění datového souboru, vyhození nosiče do odpadu). V případě získání nosiče informací a Dat je možné s vynaložením určitého úsilí informace a Data obnovit. Tato metoda není vhodná pro nosiče informací a Dat neumožňující opětovný zápis.	Nízká (Neveřejné)
Přepsání	Způsob likvidace spočívá v opakovaném přepsání informací a Dat náhodnými hodnotami. Volně dostupné nástroje neumožňují obnovení po násobném přepsání informací a Dat. Přepsání může být nahrazeno nebo kombinováno s bezpečnou likvidací kryptografických klíčů k zašifrovaným informacím a Datům. Tato metoda není vhodná pro poškozené nosiče, nosiče neumožňující opětovný zápis, případně pro nosiče s velkou paměťovou kapacitou.	Nízká (Neveřejné) Střední (Pro vnitřní potřebu)
Fyzická likvidace	Způsob likvidace spočívající ve zničení nosiče informací a Dat, popřípadě v rozebrání nosiče a následného zničení (například mechanickým, či chemickým působením vč. tepelného). Nosič informací a Dat po fyzické likvidaci nelze znovu použít. Informace a Data není možné z tohoto nosiče obnovit ani při vynaložení značného množství prostředků a úsilí.	Nízká (Neveřejné) Střední (Pro vnitřní potřebu) Vysoká a kritická (Chráněné)

25. ZÁVĚREČNÁ UJEDNÁNÍ

25.1 Smluvní strany se zavazují postupovat v souladu s relevantními obecně závaznými právními předpisy.

25.2 Dodavatel se zavazuje postupovat v souladu s bezpečnostními politikami, které mu budou Objednatelem zpřístupněny.

25.3 Dodavatel se zavazuje přenést na jakéhokoli poddodavatele, který bude schválen Objednatelem, ujednání k zajištění kybernetické bezpečnosti uvedené ve Smlouvě a v této Příloze v rozsahu, který je relevantní pro plnění poskytovaná daným poddodavatelem a tato ujednání nesmí být v rozporu s požadavky uvedenými ve Smlouvě a v této Příloze.

25.4 Dodavatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy a zajistit ve spolupráci s Objednatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční nebo efektivní.

25.5 Pokud není ve Smlouvě nebo v této Příloze uvedeno jinak, odměna za provádění povinností a opatření dle této Přílohy je součástí odměny dle Smlouvy.

25.6 Čl. 24 této Přílohy se uplatní podpůrně s ohledem na čl. 23 Smlouvy.

PŘÍLOHA Č. 7 CENÍK

Název veřejné zakázky: Konfigurace a implementace bezpečnostních funkcí prostředí Microsoft			
Soupis cen			
Část plnění	Cena bez DPH	DPH	Cena včetně DPH
Konfigurace a implementace v testovacím prostředí dle technické specifikace	1 361 600,00 Kč	285 936,00 Kč	1 647 536,00 Kč
Konfigurace a implementace v samotném systému dle technické specifikace	888 000,00 Kč	186 480,00 Kč	1 074 480,00 Kč
Celková nabídková cena	2 249 600,00 Kč	472 416,00 Kč	2 722 016,00 Kč

PŘÍLOHA Č. 8 VZOR AKCEPTAČNÍHO PROTOKOLU

(Samostatní volná příloha Smlouvy)

Technická specifikace předmětu plnění

VZMR „Konfigurace a implementace bezpečnostních funkcí prostředí Microsoft“ projektu „Posílení kybernetické bezpečnosti Úřadu městské části Praha 14“

1. Úvod a metodika

Tento dokument definuje závaznou technickou specifikaci předmětu plnění pro realizaci bezpečnostních a provozních opatření v hybridním prostředí Zadavatele (on-premises + Microsoft 365/Azure AD). Dokument je určen pro plnění veřejné zakázky a stanovuje jednotnou metodiku, očekávané výstupy, akceptační kritéria a relevantní normy a standardy. Cílem je zvýšení úrovně kybernetické odolnosti, sjednocení správy a dosažení měřitelných zlepšení bezpečnostní pozice včetně zvýšení Microsoft Secure Score.

Metodika a pořadí kroků: Pro každé opatření se postupuje konzistentně v následujících fázích: (1) Analýza a návrh, včetně identifikace rizik (ISO/IEC 27005) a dopadů; (2) Zřízení a ověření v izolovaném testovacím prostředí na infrastruktuře Hyper-V Zadavatele; (3) Pilot a postupná implementace do produkčního prostředí s řízením změn; (4) Dokumentace, předávací protokol a zaškolení. Dílčí kroky budou řízeny zásadami Zero Trust (NIST SP 800-207) a doporučeními CIS Benchmarks.

Normativní rámec: Implementace se opírá zejména o ISO/IEC 27001 a 27002 (řízení a katalog opatření), ISO/IEC 27005 (řízení rizik), ISO/IEC 27035 (řízení incidentů), NIST SP 800-53 (bezpečnostní kontroly), NIST SP 800-63-3 (identita a MFA), CIS Benchmarks (Windows Server/Windows 11/Active Directory/Microsoft 365/Intune), Microsoft Security Baselines, Microsoft Privileged Access Model (Enterprise Access Model), MITRE ATT&CK a pro PKI o RFC 5280 a RFC 3647. Opatření budou realizována tak, aby neomezila klíčové funkcionality a aby byla prokazatelně ověřena na testovacím prostředí před produkčním nasazením.

1) Analýza stávajícího hybridního prostředí Zadavatele

Úvod: Úvod: Účelem analýzy je získat ucelený, přesný a ověřitelný obraz současného stavu on-premises a cloudových komponent (Active Directory, Azure AD/Microsoft Entra ID, Microsoft 365, síť, koncové body, e-mail, správa zranitelností a logování). Analýza stanoví výchozí bezpečnostní pozici, identifikuje rizika a technické dluhy a připraví podklad pro návrh opatření. Východiskem jsou principy ISMS dle ISO/IEC 27001/27002, řízení rizik dle ISO/IEC 27005 a rámec NIST CSF.

Specifikace: Specifikace: Bude provedena inventarizace identit a rolí, GPO a AD objektů, doménových služeb, síťové topologie, hranic důvěry, protokolů, aplikací a integračních bodů. Dále se provede sběr konfigurací Microsoft 365 (Exchange Online, SharePoint/OneDrive, Teams, Defender, Intune), audit připojených zařízení, vyhodnocení logování (Windows Advanced Audit Policy, M365 audit), baseline Microsoft Secure Score a CIS (M365,

Windows/AD). Výstupem je AS-IS dokumentace (diagramy, exporty, rizika s prioritou a dopadem) a návrh testovacích scénářů a pilotních skupin.

Akceptace: Akceptace: Předmětem akceptace je AS-IS zpráva s diagramy a exporty konfigurací, seznam rizik s kategorizací a prioritizací (ISO/IEC 27005), inicializační měření Secure Score a přehled CIS odchylek. Součástí je schválený plán testovacích scénářů a pilotních skupin, včetně harmonogramu a metrik. Akceptace proběhne podpisem předávacího protokolu s přílohami (exporty, výpisy, screenshoty).

2) Vytvoření virtuálního testovacího prostředí na Hyper-V infrastruktuře Zadavatele (1× DC, 1× member server, 1× Windows 11)

Úvod: Úvod: Cílem je zřídit izolované, reprodukovatelné a checkpointované testovací prostředí pro ověřování změn bez dopadu na produkci. Testovací lab musí věrně reprezentovat klíčové aspekty produkčního prostředí (identita, síť, zásady) a umožnit regresní testy. Vychází se z osvědčených postupů řízení změn (ITIL/ISO 27001) a hardeningu dle CIS Benchmarks.

Specifikace: Specifikace: Na existující Hyper-V infrastruktuře bude vytvořena oddělená virtuální síť s vnitřní DNS/DHCP (je-li potřeba) a třemi VM: doménový řadič (nejnovější podporovaná verze Windows Server), členský server (aplikace/souborové služby) a klient s Windows 11. Budou nastaveny integrace (timetable sync, zálohy, checkpointy), přeneseny vzorové politiky a data v bezpečně anonymizované podobě, definovány testovací účty a skupiny. Bude připraven běhový Runbook pro rychlé znovuvytvoření a obnova labu.

Akceptace: Akceptace: Dodán popis architektury labu, seznam VM a parametrů (CPU/RAM/disky/sítě), export Hyper-V konfigurací, přístupové údaje testovacích účtů a Runbook. Všechny VM musí být spustitelné, přihlásitelné a vzájemně dosažitelné s funkční DNS/AD. Součástí je úspěšné provedení sady ověřovacích testů (join do domény, GPO aplikace, základní síťová komunikace) a podpis předávacího protokolu.

3) Hardening Active Directory – revize domény, politik hesel, logování, zakázání zastaralých protokolů, revize GPO

Úvod: Úvod: Active Directory je kritická infrastrukturní služba a primární cíl útočníků. Cílem hardeningu je snížit útokovou plochu, posílit autentizaci a auditní stopu a odstranit zastaralé či zranitelné konfigurace. Opatření vychází z CIS Benchmarks (Windows/AD), Microsoft Security Baselines, NIST SP 800-53 (AC, IA, AU) a mapování MITRE ATT&CK.

Specifikace: Specifikace: Bude upravena doménová a lokální bezpečnostní politika (hesla, uzamykání, minimální délka/pass-phrases, historie, fine-grained policies). Zákaz LM/NTLMv1 a restrikce NTLM, povolení LDAP signing a channel binding, SMB signing, zákaz WDigest; povolení Kerberos AES a ochrana LSASS. Aktivace a kalibrace Advanced Audit Policy (události změn v AD, přístupy k objektům, Kerberos). Revize a konsolidace GPO

(odstranění duplicit, WMI filtrů bez využití, vyčištění nastavení), nasazení Microsoft Security Baselines pro DC a členské stanice. Nasazení Windows LAPS pro správu lokálních hesel. Validace replikace AD, DNS a SYSVOL.

Akceptace: Akceptace: Předloženy zálohy a exporty GPO před/po, přehled změn, seznam zakázaných protokolů a ověřovací výpisy (např. efektivní nastavení „Network security: LAN Manager authentication level", LDAP signing). Doloženy záznamy z auditních logů po pilotu, report CIS odchylek po hardeningu a výsledky RSOP/GPResult. Akceptace proběhne na základě protokolu s evidencí testů a schválením změn.

4) Nasazení TIER modelu pro správcovské a servisní účty

Úvod: Úvod: Cílem TIER/EAM modelu je striktně oddělit privilegované přístupy do úrovní (Tier 0 – řadiče domény a kritická identita, Tier 1 – servery/aplikace, Tier 2 – klienti) a zabránit laterálnímu pohybu. Model navazuje na Microsoft Privileged Access Model / Enterprise Access Model a principy Zero Trust.

Specifikace: Specifikace: Zřídí se samostatné administrátorské identity, skupiny a OU pro každou úroveň. Budou nasazeny logon restrictions (Deny log on…/Allow log on…), Authentication Policies/Policy Silos pro Tier 0, dedikované Privileged Access Workstations (PAW) a skokové servery. Nastaví se JEA (Just Enough Administration) tam, kde je to možné, a oddělí se servisní účty s přísnými Kerberos keytab/managed identity pravidly. Vznikne katalog systémů podle TIER s mapou přístupů a pravidly pro schvalování a revize.

Akceptace: Akceptace: Dodána dokumentace mapování TIER, seznam administrátorských účtů a jejich omezení, konfigurační výpisy GPO a Authentication Policies. Provede se praktická zkouška, že přihlášení z nižšího TIER do vyššího je blokováno a že privilegované akce lze provádět pouze z PAW. Akceptace bude potvrzena protokolem s výsledky testů a výpisy z auditních logů.

5) Konfigurace a nasazení Conditional Access Policy v rámci M365 pro všechny uživatele

Úvod: Úvod: Conditional Access (CA) uplatňuje zásady „ověř, než povolíš" a je klíčovým prvkem Zero Trust. Cílem je vynutit vícefaktor, podmínit přístup stavem zařízení, rizikem přihlášení a umístěním a současně zachovat obchodní funkčnost. Opatření vychází z NIST SP 800-63-3 (AAL), NIST SP 800-207 a Microsoft doporučení.

Specifikace: Specifikace: Bude navržena a nasazena sada politik: zákaz legacy authentication, vyžadování MFA pro všechny, vynucení compliant/Hybrid-joined zařízení pro citlivé aplikace, pojmenované lokace, řízení přístupu pro externí uživatele, session controls (token lifetime, sign-in frequency), Terms of Use. Budou definovány výjimky pro „break-glass" účty, pilotní skupiny a staged rollout. Politiky budou testovány v simulátoru CA a na labu, poté nasazeny postupně podle rizika.

Akceptace: Akceptace: Dodán export politik (JSON), matice přístupových scénářů a výsledky testů (sign-in logs). Ověřeno blokování legacy auth a vynucení MFA/Device compliance podle očekávání v pilotu i produkci. Akceptace potvrzena protokolem s evidencí výjimek a jejich odůvodnění.

6) Audit a hardening M365 tenantu na základě CIS doporučení

Úvod: Úvod: Cílem je harmonizovat nastavení Microsoft 365 s CIS Benchmarks a Microsoft Security Baselines a snížit rizika spojená se sdílením, e-mailem, aplikacemi a přístupem třetích stran. Tím se zvyšuje Secure Score a zajišťuje konzistence nastavení napříč službami.

Specifikace: Specifikace: Provede se CIS gap analýza a úpravy: Exchange Online (antispam/anti-phishing/impersonation, zakázání auto-forwardu), SharePoint/OneDrive/Teams (externí sdílení, expirační pravidla, guest access), Azure AD/Entra (admin role, audit, consent/consent workflow, registrace aplikací), aktivace a kalibrace „Unified Audit Log“. Nasadí se DKIM a DMARC pro ověřené domény, nastaví se bezpečnostní výstrahy a integrace s Defenderem.

Akceptace: Akceptace: Předložen report CIS s vyřešenými odchylkami, export nastavení (Exchange Online, SharePoint, Azure AD), důkaz o zapnutí DKIM/DMARC, kontrola Unified Audit Log a vzorové alerty. Akceptační protokol bude obsahovat seznam aplikovaných doporučení a jejich dopad na Secure Score.

7) Nasazení Defender for Office 365 – Safe Attachments a Safe Links, karanténa a anti-spam

Úvod: Úvod: Cílem je omezit riziko phishingu a malwaru v e-mailu a spolupráci. Safe Attachments a Safe Links poskytují detonaci příloh a kontrolu odkazů v reálném čase, centralizovaná karanténa a anti-spam politiky řízenou reakci. Opatření navazuje na NIST SP 800-177 (e-mail) a kontrolní rodiny NIST SP 800-53 (SI, SC).

Specifikace: Specifikace: Aktivace Safe Attachments (preferováno „Dynamic Delivery“) a Safe Links pro Exchange Online, Teams a SharePoint/OneDrive, konfigurace impersonation protection (domény/uži-va-telé), vrácení zpráv z karantény s dvojím schválením, zásady pro high-confidence phishing (default „Quarantine“), pravidla pro antispam a anti-malware, notifikace uživatelům a SOC. Nastaví se reporty a playbooky reakce.

Akceptace: Akceptace: Doloženy snapshoty politik, testy s GTUBE (spam) a kontrolními odkazy Safe Links v labu, záznamy o karanténě a statistikách. Ověřena účinnost politik dle definovaných scénářů. Akceptace potvrzena protokolem s přehledem zásahů a povolených výjimek.

8) MDM – Intune: konfigurace a on-boarding zařízení, centrální správa, compliance a konfigurační politiky, aplikační balíčky, Autopilot

Úvod: Úvod: Jednotná správa koncových zařízení minimalizuje rizika a provozní náklady. Intune umožňuje vynutit bezpečnostní standardy a automatizovat onboarding přes Autopilot. Opatření vychází z CIS Benchmarks pro Intune a Windows 11 a NIST SP 800-124 (mobilní zařízení).

Specifikace: Specifikace: Zřídí se registrace zařízení (Windows 11, případně iOS/Android), nastaví se compliance politiky (BitLocker, TPM/Secure Boot, minimální verze OS, Defender, firewall), konfigurační profily (security baselines, hardening), distribuují se Win32/MSIX balíčky a Microsoft 365 Apps. Nasadí se Autopilot (zachycení HW hash, profily, pre-provisioning), vytvoří se dynamické skupiny, reporting a RBAC pro delegovanou správu.

Akceptace: Akceptace: Doloženy přehledy „Device compliance“ a „Configuration profiles“ s cílovým stavem, úspěšná Autopilot instalace na vzorových zařízeních a exporty politik. Potvrzena schopnost vzdálené akce (wipe, retire) na testovacím zařízení. Akceptace protokolem s přílohami (reporty, screenshoty).

9) Konfigurace a nasazení Microsoft Defender for Endpoint

Úvod: Úvod: MDE poskytuje EDR/XDR schopnosti, správu zranitelností a pravidla pro redukci útokové plochy. Cílem je detekce a blokování útoků, viditelnost a reakce v koncových bodech, mapování na MITRE ATT&CK.

Specifikace: Specifikace: Onboarding zařízení přes Intune/GPO, zapnutí EDR v režimu „block mode“, povolení Tamper Protection, Attack Surface Reduction (ASR) pravidel, Network Protection a Web Filtering. Aktivace Vulnerability Management, baseline politik pro servery/stanice, integrace alertů do SOC kanálů a definice reakčních playbooků (Live Response).

Akceptace: Akceptace: V portálu Defender jsou viditelná onboardovaná zařízení se stavem „Healthy“, povolený block mode a ASR pravidla. Provedeny simulační testy (bezpečné scénáře doporučené výrobcem) na testovacích stanicích a doloženy záznamy o detekci/blokování. Akceptační protokol obsahuje export politik a reporty zranitelností po remediaci.

10) Revize privilegovaných rolí a nasazení PAM (Privileged Access Management) a JIT (Just-In-Time)

Úvod: Úvod: Cílem je minimalizovat trvalá privilegia a zavést časově omezené, schvalované zvýšení oprávnění. V cloudu bude využit PIM pro role a skupiny, on-prem přístup je limitován TIER modelem, JEA a řízenými skupinami. Opatření navazuje na NIST SP 800-53 (AC-2, AC-6), Zero Trust a Microsoft EAM.

Specifikace: Specifikace: Nasadí se Azure AD/Entra PIM pro privilegované role a skupiny (approval, justification, MFA, logging, notifications), nastaví se časové okno a automatická expirace. Pro on-prem AD se zavedou řízené skupiny přístupu, JEA role pro PowerShell, omezené práva služeb a pravidelný Access Review. Definují se „break-glass" účty s monitoringem a pravidly úschovy.

Akceptace: Akceptace: Doložen seznam privilegovaných rolí, jejich PIM nastavení a auditní logy aktivací/deaktivací. Ověřena funkčnost schvalování a automatických expirací na pilotních účtech. Akceptace protokolem včetně exportu Access Reviews a seznamu „break-glass" účtů s ochranami.

11) Konfigurace štítkování a DLP pravidel (Microsoft Purview Information Protection)

Úvod: Úvod: Klasifikace a ochrana dat omezuje neúmyslné i úmyslné úniky informací. Cílem je definovat sadu citlivostních štítků a DLP politik napříč Exchange, SharePoint/OneDrive a Teams, s automatizací a auditovatelností. Vychází z ISO/IEC 27001/27002 (klasifikace aktiv) a GDPR.

Specifikace: Specifikace: Definují se štítky (např. Veřejné, Interní, Důvěrné, Přísně důvěrné) s šifrováním a ochrannými akcemi (Do Not Forward, Watermark, automatická aplikace dle detekovaných vzorů). Vytvoří se DLP politiky pro PII/finanční údaje (např. čísla platebních karet, IBAN, rodné číslo) s postupnou a pak blokující akcí, výjimkami a auditním workflow. Štítky a DLP se nasadí nejprve v „test mode" s incident raporty.

Akceptace: Akceptace: Doložen seznam štítků, jejich parametry a cílení, přehled DLP politik a incidentů z pilotu. Na vzorových dokumentech jsou štítky viditelné a aplikovatelné, testovací obsah vyvolá očekávané DLP akce. Akceptace protokolem s exporty konfigurací a incident reporty.

12) Konfigurace vícefaktorového ověřování (Microsoft Authenticator, FIDO2/čipové karty) s postupným rolloutem

Úvod: Úvod: MFA zásadně zvyšuje úroveň zabezpečení identity. Cílem je povinné MFA pro všechny uživatele s preferencí silných metod (Authenticator push, FIDO2 bezpečnostní klíče, certifikátové přihlášení) a řízený rollout s minimem provozních dopadů. Opatření vychází z NIST SP 800-63-3 (AAL2+).

Specifikace: Specifikace: Zapne se „combined registration", nastaví se povolené MFA metody (Authenticator, FIDO2, certifikátové přihlášení – Azure AD CBA), omezí se SMS/voice na krizové scénáře. CA politiky budou vyžadovat MFA dle rizika a citlivosti aplikace. Připraví se návody pro uživatele, registrační kampaň, pilotní skupiny, fallback scénáře a „break-glass" účty. U čipových karet se nastaví mapování certifikátů a validace řetězce důvěry.

Akceptace: Akceptace: Sign-in logy prokazují vynucení MFA, uživatelé v pilotu mají úspěšně zaregistrované metody a přihlášení probíhá dle scénářů. Doloženy exporty nastavení MFA a CA, seznam výjimek s odůvodněním. Akceptace protokolem po úspěšném pilotu i produkčním nasazení.

13) Kompletní konfigurace interní certifikační autority (PKI)

Úvod: Úvod: Interní PKI poskytuje důvěru pro zařízení, uživatele a služby (TLS, podpis, šifrování, CBA). Cílem je navrhnout bezpečnou dvouvrstvou architekturu a provozní postupy odpovídající RFC 5280 a RFC 3647.

Specifikace: Specifikace: Návrh a zřízení offline kořenové CA a online vydavatelské CA (AD CS), definice CP/CPS, CRL a AIA přes HTTP, OCSP responder, bezpečné šablony (Computer, User, Web Server – SAN, Client Authentication, případně Code Signing), klíče RSA 3072+ s HSM (je-li k dispozici), auto-enrollment přes GPO. Zajištění záloh, rotace klíčů, dokumentace pro obnovu a bezpečné uložení root klíče.

Akceptace: Akceptace: Doložen CP/CPS dokument, konfigurace CA (snímek konzole, certutil výpisy), funkční publikace CRL/AIA/OCSP, automatické vydání certifikátů klientům v pilotu a následně v produkci. Akceptace protokolem s testy vzájemné důvěry (TLS, smime/cba) a sepsanými havarijními postupy.

14) Revize WSUS

Úvod: Úvod: Správa aktualizací je klíčová pro eliminaci zranitelností. Cílem je nastavit konzistentní proces schvalování, kategorie a reporting pro servery i stanice a zvážit přechod na Windows Update for Business pro klientská zařízení. Opatření navazuje na ISO/IEC 27002:2022 (řízení technických zranitelností).

Specifikace: Specifikace: Provede se audit WSUS (čistota databáze, jazyky, kategorie, pravidla schvalování, reporting), vytvoří se pre-prod a prod kroužky, úklid nepoužívaných klasifikací a superseded aktualizací, nastavení SSU/LCU, optimalizace DB („WSUS Cleanup“). Pro klienty bude preferován WUfB/Intune s deferrals a deadline; servery mohou zůstat na WSUS s řízenými schváleními. Nastaví se GPO a reporty shody.

Akceptace: Akceptace: Doloženy reporty shody (compliance) z WSUS/WUfB, popisy kroužků a časových oken, evidence úspěšných aktualizací na vzorcích serverů a stanic. Akceptace protokolem s exporty konfigurací a plánem údržby WSUS.

15) Update prostředí na poslední verzi Windows Active Directory, Domain Functional Level a Forest Functional Level

Úvod: Úvod: Navýšení funkčních úrovní domény a lesa přináší bezpečnostní i provozní vylepšení. Cílem je bezpečně přejít na nejnovější podporované úrovně po odstranění technických překážek a ověření kompatibility.

Specifikace: Specifikace: Ověří se podporované verze všech DC, zdraví replikace a SYSVOL (případná migrace FRS→DFSR). Provede se záloha „system state", validace schématu, odstranění legacy DC a postupné povýšení úrovní v testu a poté v produkci. Součástí je plán údržby, okno pro změnu a rollback plán. Po aktualizaci proběhne kontrola událostí a konzistence AD.

Akceptace: Akceptace: Doloženy výpisy cílových DFL/FFL a schéma verze, protokoly replikace bez chyb, seznam aktivních DC po změně a výstup kontroly SYSVOL. Akceptace protokolem po úspěšných ověřovacích testech přihlášení a GPO aplikace.

16) Zpracování podrobné dokumentace o realizaci plnění včetně předávacího protokolu

Úvod: Úvod: Dokumentace zajišťuje přenos know-how a auditní stopu. Předávací protokol formálně potvrzuje splnění a převzetí. Dokumentace navazuje na požadavky ISMS a ITIL Service Transition.

Specifikace: Specifikace: Budou dodány architektonické diagramy, konfigurace (exporty), Runbooky, provozní postupy (incident/změna/problém), katalog rizik a výjimek, testovací scénáře a jejich výsledky, seznam účtů/rolí a mapování TIER, CP/CPS pro PKI, školící materiály. Vše ve strojově čitelných formátech (CSV/JSON/XML) i v čitelné podobě (PDF/DOCX).

Akceptace: Akceptace: Předávací protokol bude obsahovat kontrolní seznam všech výstupů, verzování a umístění v repozitáři Zadavatele. Akceptace proběhne po kontrole úplnosti, čitelnosti a úspěšném provedení vzorových postupů z Runbooků.

17) Zvýšení Microsoft Secure Score z ≈44 % na >85 % při zachování klíčových funkcionalit

Úvod: Úvod: Secure Score je kvantitativní metrika bezpečnostní pozice v Microsoft 365. Cílem je dosažení stavu >85 % pomocí prioritizovaných opatření, bez negativního dopadu na klíčové procesy. Secure Score je mapován na průmyslové standardy (NIST, ISO).

Specifikace: Specifikace: Budou implementována opatření s nejvyšší váhou: plošné MFA, blokace legacy auth, Conditional Access, MDE (EDR/ASR), Safe Links/Attachments, DLP/štítkování, hardening sdílení a správy aplikací, role-based access a audit. Před

nasazením proběhne analýza dopadů a pilot. Nezbytné výjimky budou dokumentovány s kompenzačními kontrolami a pravidelným přezkumem.

Akceptace: Akceptace: Doložen export Secure Score (CSV/PDF) před a po, aktuální hodnota >85 % v den akceptace, seznam zbývajících doporučení s odůvodněnými výjimkami a plánem jejich řešení. Potvrzeno UAT, že klíčové funkcionality zůstaly zachovány.

18) Zaškolení vybraných pracovníků Zadavatele a outsourcera (max. 10 osob, rozsah 2 člověkodny)

Úvod: Úvod: Cílem školení je předat znalosti pro provoz a rozvoj implementovaných opatření a zvýšit schopnost týmu reagovat na incidenty. Školení kombinuje teorii a praktická cvičení v testovacím prostředí.

Specifikace: Specifikace: Sylabus zahrnuje: AD hardening a TIER/EAM, Conditional Access a MFA, M365 hardening (CIS), Defender for Office 365 a MDE (reakce na incident), Intune (compliance, Autopilot), PKI (CP/CPS, provoz). Poskytnuty materiály (prezentace, runbooky, checklisty), lab návody a odpovědi na dotazy.

Akceptace: Akceptace: Předložen prezenční list, krátký znalostní test a evaluační dotazník s průměrným hodnocením ≥4/5. Materiály budou předány v elektronické podobě. Akceptace proběhne podpisem protokolu o zaškolení.

Souhrnná tabulka norem a standardů

Oblast	Norma / standard	Rozsah použití	Použito u bodů
Řízení bezpečnosti informací	ISO/IEC 27001:2022	ISMS a vazby na opatření	1–18
Katalog kontrol	ISO/IEC 27002:2022	Kontroly (zejm. 5.34, 8.8, 8.9, 8.15, 8.16)	1–18
Řízení rizik	ISO/IEC 27005	Identifikace a hodnocení rizik	1, 6, 16
Incident management	ISO/IEC 27035	Řízení incidentů a lekce learned	9, 16
Zero Trust	NIST SP 800-207	Architektonické principy	4, 5, 9, 10, 12
Identita a MFA	NIST SP 800-63-3	AAL úrovně a MFA/CBA	5, 10, 12

Bezpečnostní kontroly	NIST SP 800-53 Rev. 5	Kontroly AC, IA, AU, SI	3–12
Log management	NIST SP 800-92	Auditní záznamy a jejich správa	3, 6
CIS Benchmarks	CIS (Windows Server, Windows 11, AD, Microsoft 365, Intune)	Hardening a auditní body	2–11, 14, 15
Microsoft Baselines	Security Baselines (Windows/Server/M365 Apps/Edge)	Referenční konfigurační zásady	3, 8, 9, 11, 12, 14
Privilegovaný přístup	Microsoft EAM/PAM, JEA	TIER/EAM, JIT/JEA	4, 10
PKI	RFC 5280, RFC 3647, (ETSI EN 319 411-1/2 – informativně)	Profil certifikátů, CP/CPS	13, 12
E-mail	NIST SP 800-177, SPF/DKIM/DMARC (RFC 7208/6376/7489)	Zabezpečení e-mailu	6, 7
Ochrana osobních údajů	GDPR – Nařízení (EU) 2016/679	Zpracování osobních údajů	6, 11, 12
Patch management	ISO/IEC 27002:2022 – 8.8, 8.9	Zranitelnosti a změny	14, 15
Detekční rámec	MITRE ATT&CK (Enterprise)	Mapování detekcí/ASR	3, 9
Metrika	Microsoft Secure Score	Měření bezpečnostní pozice	17

Příloha č. 8 smlouvy

Kontrolní seznam akceptačních kritérií technických opatření

Zadavatel	_____
Dodavatel	_____
Název zakázky	_____
Číslo smlouvy/objednávky	_____
Kontaktní osoby	Zadavatel: _____ | Dodavatel: _____
Místo plnění	_____

Legenda stavu: ☐ Splněno ☐ Částečně ☐ Nesplněno ☐ N/A

Každé kritérium je možné doložit odkazem na soubor či dokument (interní úložiště, SharePoint, ticket, export).

1) Analýza stávajícího hybridního prostředí Zadavatele

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
1.1	AS-IS zpráva včetně diagramů on-prem a M365/Entra komponent.	—	—	☐	—	—
1.2	Seznam rizik s kategorizací dle ISO/IEC 27005 a prioritizací dopadů.	—	—	☐	—	—
1.3	Výchozí hodnota Microsoft Secure Score – export (CSV/PDF).	—	—	☐	—	—
1.4	CIS gap analýza (M365, Windows/AD) – seznam odchylek.	—	—	☐	—	—
1.5	Plán testovacích	—	—	☐	—	—

	scénářů a pilotních skupin (včetně metrik).					
1.6	Schválený harmonogram realizace a řízení změn.	—	—	□	—	—

2) Vytvoření virtuálního testovacího prostředí na Hyper-V (1× DC, 1× member server, 1× Windows 11)

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
2.1	Topologie a izolace testovací sítě v Hyper-V (vSwitch, VLAN dle potřeby).	—	—	☐	—	—
2.2	Seznam VM s parametry (CPU/RAM/Disk/Síť) a OS verzemi.	—	—	☐	—	—
2.3	Export konfigurací Hyper-V a zřízené checkpointy/backupy.	—	—	☐	—	—
2.4	Založené testovací účty, skupiny a vzorová data (anonymizovaná).	—	—	☐	—	—
2.5	Runbook pro vytvoření/obnovu labu krok za krokem.	—	—	☐	—	—
2.6	Ověřovací testy: join do domény, aplikace GPO, DNS/DHCP konektivita.	—	—	☐	—	—

3) Hardening Active Directory (doména, hesla, audit, protokoly, GPO)

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
3.1	Změny doménové/lokální politiky hesel (vč. FGPP) – export nastavení.	—	—	☐	—	—
3.2	Zákaz LM/NTLMv1, restrikce NTLM; LDAP signing a channel binding.	—	—	☐	—	—
3.3	SMB signing; ochrana LSASS; zákaz WDigest; Kerberos AES povolen.	—	—	☐	—	—
3.4	Advanced Audit Policy – aktivace a kalibrace sledovaných událostí.	—	—	☐	—	—
3.5	Revize a konsolidace GPO; nasazení Microsoft Security Baselines.	—	—	☐	—	—
3.6	Nasazení	—	—	☐	—	—

	Windows LAPS pro správu lokálních hesel.					
3.7	Report CIS odchylek po hardeningu; RSOP/GPResult z pilotu.	—	—	☐	—	—

4) Nasazení TIER modelu pro správcovské a servisní účty

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
4.1	Mapování systémů do TIER 0/1/2 a dokumentace přístupových pravidel.	—	—	☐	—	—
4.2	Vytvoření admin identit, skupin a OU dle TIER; logon restrictions.	—	—	☐	—	—
4.3	Authentication Policies/Policy Silos pro TIER 0 a citlivé účty.	—	—	☐	—	—
4.4	Nasazení PAW/Jump serverů pro privilegované operace.	—	—	☐	—	—
4.5	Definice JEA (Just Enough Administration) pro vybrané role.	—	—	☐	—	—
4.6	Test: blokace	—	—	☐	—	—

	přihlášení z nižšího TIER do vyššího; auditní záznamy.					

5) Conditional Access Policy v M365 pro všechny uživatele

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
5.1	Export a přehled CA politik (JSON) – návrh a finální stav.	—	—	☐	—	—
5.2	Zákaz legacy authentication pro všechny uživatele/aplikace.	—	—	☐	—	—
5.3	Vynucení MFA; výjimky pouze pro „break-glass“ účty (dokumentováno).	—	—	☐	—	—
5.4	Podmínění přístupu stavem zařízení (compliant/hybrid joined).	—	—	☐	—	—
5.5	Pojmenované lokace a pravidla session (sign-in frequency, token lifetime).	—	—	☐	—	—
5.6	Výsledky testů v simulátoru CA a sign-in logy z pilotu.	—	—	☐	—	—

6) Audit a hardening M365 tenantu dle CIS

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
6.1	CIS gap report s vyřešenými odchylkami a reziduálními výjimkami.	—	—	☐	—	—
6.2	Exchange Online: anti-spam/anti-phishing/impersonation – konfigurace.	—	—	☐	—	—
6.3	SharePoint/OneDrive/Teams: externí sdílení a expirační pravidla.	—	—	☐	—	—
6.4	Azure AD/Entra: admin role, consent workflow, app registrations.	—	—	☐	—	—
6.5	Unified Audit Log aktivní a ověřen; ukázkové audity/alerty.	—	—	☐	—	—
6.6	DKIM a DMARC aktivní pro ověřené domény – důkaz konfigurace.	—	—	☐	—	—

7) Defender for Office 365 – Safe Attachments, Safe Links, karanténa a antispam

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
7.1	Safe Attachments aktivní (Dynamic Delivery) – zásady a scény.	—	—	☐	—	—
7.2	Safe Links pro Exchange/Teams/SharePoint/OneDrive – zásady.	—	—	☐	—	—
7.3	Impersonation protection (domény, VIP účty) – konfigurace.	—	—	☐	—	—
7.4	Karanténa: workflow schvalování a role; audit uvolnění zpráv.	—	—	☐	—	—
7.5	Anti-spam/anti-malware politiky – cílení a priority.	—	—	☐	—	—
7.6	Testy (GTUBE, kontrolní odkazy) a související reporty.	—	—	☐	—	—

8) MDM – Intune: on-boarding, centrální správa, compliance, balíčky, Autopilot

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
8.1	Registrace zařízení (Windows 11 / mobilní) do Intune – přehled.	—	—	☐	—	—
8.2	Compliance politiky (BitLocker, TPM/Secure Boot, OS verze, Defender).	—	—	☐	—	—
8.3	Konfigurační profily a Security Baselines – nasazení a výsledky.	—	—	☐	—	—
8.4	Distribuce aplikací (Win32/MSIX, Microsoft 365 Apps) – stav nasazení.	—	—	☐	—	—
8.5	Autopilot profily,	—	—	☐	—	—

	zachycení HW hash, pre-provisioning – testy.					
8.6	RBAC pro delegovanou správu a reporting compliance.	—	—	□	—	—

9) Microsoft Defender for Endpoint – nasazení a konfigurace

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
9.1	Onboarding zařízení (Intune/GPO) – seznam a stav v portálu.	—	—	☐	—	—
9.2	EDR v block mode; Tamper Protection povolena.	—	—	☐	—	—
9.3	ASR pravidla, Network Protection a Web Filtering – nastavení.	—	—	☐	—	—
9.4	Vulnerability Management aktivní – report zranitelností a remedicí.	—	—	☐	—	—
9.5	Integrace alertů do SOC kanálů; playbooky reakce (Live Response).	—	—	☐	—	—
9.6	Simulační testy detekcí/blokování – logy a výsledky.	—	—	☐	—	—

10) PAM & JIT – Privileged Access Management a Just-In-Time

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
10.1	PIM pro privilegované role/skupiny: approval, justification, MFA.	—	—	☐	—	—
10.2	Nastavené časové intervaly, expirace a notifikace.	—	—	☐	—	—
10.3	Access Reviews pro role a skupiny – exporty a výsledky.	—	—	☐	—	—
10.4	On-prem: řízené skupiny, JEA role, omezení služebních účtů.	—	—	☐	—	—
10.5	Break-glass účty definovány, monitorovány a auditovány.	—	—	☐	—	—
10.6	Auditní logy aktivací/deaktivací a test schvalovacího toku.	—	—	☐	—	—

11) Štítkování a DLP (Microsoft Purview Information Protection)

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
11.1	Definice citlivostních štítků (vč. šifrování a ochranných akcí).	—	—	☐	—	—
11.2	DLP politiky pro PII/finanční údaje s výjimkami a workflow.	—	—	☐	—	—
11.3	Nasazení v Exchange, SharePoint/OneDrive a Teams (test mode → enforce).	—	—	☐	—	—
11.4	Incident reporty z pilotu a vyhodnocení dopadů.	—	—	☐	—	—
11.5	Testy na vzorových dokumentech – očekávané akce DLP/štítků.	—	—	☐	—	—
11.6	Export konfigurací štítků a DLP politik.	—	—	☐	—	—

12) MFA – Microsoft Authenticator, FIDO2/čipové karty, postupný rollout

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
12.1	Combined registration aktivní; zásady registrace uživatelů.	—	—	☐	—	—
12.2	Povolené metody: Authenticator push, FIDO2, CBA; omezení SMS/voice.	—	—	☐	—	—
12.3	CA politiky vynucující MFA dle rizika a citlivosti aplikací.	—	—	☐	—	—
12.4	Pilotní skupiny, registrační kampaň a uživatelské návody.	—	—	☐	—	—
12.5	Break-glass účty –	—	—	☐	—	—

	pravidla, dohled a audit.					
12.6	Sign-in logy dokazující plošné vynucení MFA.	—	—	☐	—	—

13) Interní certifikační autorita (PKI)

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
13.1	Architektura PKI: offline root CA + online issuing CA (AD CS).	—	—	☐	—	—
13.2	CP/CPS dokument; schválení a verzování.	—	—	☐	—	—
13.3	Publikace CRL/AIA přes HTTP; OCSP responder funkční.	—	—	☐	—	—
13.4	Šablony certifikátů (Computer/User/Web Server/Client Auth) a auto-enrollment.	—	—	☐	—	—
13.5	Zálohy klíčů, rotace a bezpečné uložení kořenového klíče/HSM.	—	—	☐	—	—
13.6	Vydané certifikáty klientům/zařízením; test TLS, S/MIME, CBA.	—	—	☐	—	—

14) Revize WSUS

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
14.1	Audit konfigurace WSUS; cleanup databáze, jazyky a kategorie.	—	—	☐	—	—
14.2	Zřízení kroužků (pre-prod/prod) a pravidel schvalování.	—	—	☐	—	—
14.3	GPO pro WSUS/WUfB; deferrals a deadlines.	—	—	☐	—	—
14.4	Reporting shody (compliance) pro servery a stanice.	—	—	☐	—	—
14.5	Evidence úspěšných aktualizací ve vzorcích serverů/klientů.	—	—	☐	—	—
14.6	Plán údržby WSUS a dohoda odpovědností.	—	—	☐	—	—

15) Update AD na poslední DFL/FFL

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
15.1	Zálohy system state všech DC před změnou.	—	—	☐	—	—
15.2	Validace replikace a konzistence SYSVOL (DFSR, bez chyb).	—	—	☐	—	—
15.3	Odstranění legacy DC; validace schématu.	—	—	☐	—	—
15.4	Pilotní povýšení DFL/FFL v testu; výsledky kontrol.	—	—	☐	—	—
15.5	Povýšení DFL/FFL v produkci; kontrola událostí.	—	—	☐	—	—
15.6	Dokumentace	—	—	☐	—	—

	cílových verzí DFL/FFL a schéma verze.					

16) Dokumentace o realizaci a předávací protokol

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
16.1	Architektonické diagramy a konfigurační exporty.	—	—	☐	—	—
16.2	Runbooky a provozní postupy (incident/změna/problém).	—	—	☐	—	—
16.3	Katalog rizik a výjimek; seznam účtů/rolí a TIER mapování.	—	—	☐	—	—
16.4	Testovací scénáře, protokoly a výsledky.	—	—	☐	—	—
16.5	PKI CP/CPS; školící materiály.	—	—	☐	—	—
16.6	Kompletace předávacího protokolu včetně příloh.	—	—	☐	—	—

17) Zvýšení Microsoft Secure Score > 85 %

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
17.1	Export Secure Score – výchozí stav (≈44 %).	—	—	☐	—	—
17.2	Implementovaná opatření s nejvyšší vahou (MFA, CA, MDE, DLP, Safe Links/Attachments).	—	—	☐	—	—
17.3	Export Secure Score – cílový stav (>85 %) v den akceptace.	—	—	☐	—	—
17.4	Seznam výjimek a kompenzačních kontrol; plán přezkumu.	—	—	☐	—	—
17.5	UAT potvrzení zachování klíčových funkcionalit.	—	—	☐	—	—

18) Zaškolení (max. 10 osob, 2 člověkodny)

ID	Akceptační kritérium	Důkaz/Dokumenty (soubor/odkaz)	Způsob naplnění / Poznámka	Stav (☐/☐/☐/☐)	Kontroloval	Datum
18.1	Prezenční list účastníků (Zadavatel + outsourcer).	—	—	☐	—	—
18.2	Sylabus školení a agenda.	—	—	☐	—	—
18.3	Školící materiály (prezentace, runbooky, checklisty).	—	—	☐	—	—
18.4	Praktická lab cvičení; návody.	—	—	☐	—	—
18.5	Znalostní test a vyhodnocení; průměrné skóre ≥ 4/5.	—	—	☐	—	—
18.6	Evaluační dotazník účastníků a závěrečné Q&A.	—	—	☐	—	—

Seznam příloh a důkazních materiálů

Ref	Název souboru	Umístění (odkaz/úložiště)	Související kritéria (ID)	Poznámka
P01	—	—	—	—
P02	—	—	—	—
P03	—	—	—	—
P04	—	—	—	—
P05	—	—	—	—
P06	—	—	—	—
P07	—	—	—	—

Výjimky a otevřené body

ID kritéria	Popis výjimky/otevřeného bodu	Kompenzační opatření	Zodpovědnost	Termín uzavření
—	—	—	—	—
—	—	—	—	—
—	—	—	—	—
—	—	—	—	—
—	—	—	—	—

Rekapitulace plnění

Ukazatel	Počet kritérií	Počet splněných	Poznámka
Celkem (všechny body)	—	—	—
Částečně splněno	—	—	—
Nesplněno/N/A	—	—	—

Podpisy a převzetí plnění

Za Zadavatele	**Za Dodavatele**
Jméno a příjmení: Funkce: Datum: Podpis:	Jméno a příjmení: Funkce: Datum: Podpis:
Razítko (je-li používáno)	Razítko (je-li používáno)