Národní plán obnovy

Financováno Evropskou unií NextGenerationEU

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

PŘÍLOHA č. 1

ŽÁDOST O FINANČNÍ PODPORU NPO

pro komponenty 1.1, 1.2 a 4.4

Bezpečná infrastruktura Města Znojma

1. Základní informace o projektu

1.1. Identifikační údaje žadatele o finanční podporu

Žadatel - konečný příjemce (instituce)	Město Znojmo
IČ žadatele	00293881
Adresa žadatele	Obroková 1/12, 669 02 Znojmo
Číslo bankovního účtu žadatele	94-1411741/0710
Typ plátce DPH	jsem plátcem DPH a nemám nárok na odpočet DPH ve vztahu k aktivitám projektu
Správce rozpočtové kapitoly (instituce)	Ministerstvo vnitra ČR
Ředitel projektu	Ing. et Ing. Růžena Salvetová, oddělení strategického rozvoje a dotací, 733 781 603, ruzena.salvetova@muznojmo.cz
Statutární zástupce organizace	Mgr. František Koudela, starosta, 515 216 250, frantisek.koudela@muznojmo.cz
Projektový manažer	Ing. et Ing. Růžena Salvetová, oddělení strategického rozvoje a dotací, 733 781 603, ruzena.salvetova@muznojmo.cz
Odborný gestor (věcná odbornost)	Ing. Lubomír Otepka, vedoucí oddělení informatiky, 603 888 385, lubomir.otepka@muznojmo.cz
Technický gestor (technická odbornost)	Ing. Lubomír Otepka, vedoucí oddělení informatiky, 603 888 385, lubomir.otepka@muznojmo.cz

1.2. Základní údaje

Název projektu CZ	**Bezpečná infrastruktura Města Znojma**		
Název projektu EN	**Secure infrastructure of the city of Znojmo**		
Předpokládané zahájení projektu (dd. mm. rrrr)	1.9.2023	**Předpokládané ukončení projektu (dd. mm. rrrr)**	31.5.2026
Předmět projektu (max. 500 znaků)	Aktivity realizované v rámci tohoto projektu si kladou za cíl zabezpečit a modernizovat územní veřejnou správu prostřednictvím zavedení prvků kybernetické bezpečnosti do systémů využívaných městem Znojmem.		
Celkové způsobilé výdaje projektu, financované v rámci NPO (bez DPH)	24 787 320 Kč bez DPH		
Celkové výdaje projektu (vč. DPH)	29 904 457 Kč s DPH		

Odůvodnění potřebnosti projektu	Projekt je realizován za účelem ochrany a zabezpečení důležitých dat a důležitých služeb poskytovaných v rámci informačních systémů (IS) a provozovaných v rámci komunikačních systémů (KS) města Znojmo s cílem zachování a zajištění jejich důvěrnosti, integrity a dostupnosti. Proto je nezbytné implementovat dosud nezavedené nástroje kybernetické bezpečnosti v oblasti bezpečnosti komunikačních sítí, autentizace uživatelů, administrátorů a aplikací, řízení přístupů (administrátorů a uživatelů), zaznamenávání a archivaci bezpečnostních událostí, detekci bezpečnostních událostí a incidentů, aplikační bezpečnosti a doplnit tak dosavadní částečně zavedená bezpečnostní základní technická opatření v oblasti fyzické bezpečnosti, ochraně proti škodlivému kódu a bezpečnosti komunikačních síti.
Cíl projektu	Hlavního cíle předkládaného projektu bude dosaženo prostřednictvím modernizace stávajících kyberbezpečnostních opatření města za účelem zvýšení spolehlivé efektivnosti územní veřejné správy a vytvořit podmínky pro zvýšení kvality a transparentnosti služeb poskytovaných veřejnou správou v rámci samosprávných agend. rozvoj, modernizace a zvýšení dostupnosti komunikačních a informačních systémů a infrastruktury. - budování, rozvoj a modernizace zabezpečených regionálních datových center a komunikační infrastruktury pro modernizované informační systémy; - vytváření bezpečného prostředí pro provoz služeb úřadu, včetně bezpečného přístupu zaměstnanců; - modernizace stávajících podpůrných informačních systémů.
Očekávaný přínos (přínosy) projektu	Dopady a přínosy projektu na cílové skupiny: • instituce veřejné správy (MěÚ Znojmo) - zabezpečení ochrany ICT vybavení, technických aktiv a služeb MěÚ, • zaměstnanci ve veřejné správě (úředníci MěÚ Znojmo) - zajištění bezpečné komunikace a práce s daty pro úředníky v rámci MěÚ, • občané (občané spádové oblasti města Znojmo I) - zabezpečení dat/údajů o občanech a poskytovaných služeb pro občany, • podnikatelské subjekty (podnikatelé spádové oblasti města - (zabezpečení dat/údajů o podnikatelích a poskytovaných služeb pro podnikatele)
Návaznost na strategii (strategické cíle)	Program Digitální Česko – Informační Koncepce ČR, Hlavní cíl 3: Rozvoj prostředí podporujícího digitální technologie v oblasti eGovernmentu, Dílčí cíl 3.8: Podpora opatření kybernetické bezpečnosti pro veřejnou správu. Soulad s cíli Informační koncepce České republiky: Kybernetická bezpečnost - realizace technických bezpečnostních opatření podle § 5 odst. 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a mezinárodních standardů a norem v oblasti bezpečnosti informací. Cíl č. 1 „Uživatelsky přívětivé a efektivní on-line služby pro občany a firmy“ Cíl č. 3 „Rozvoj prostředí podporujícího digitální technologie v oblasti eGovernmentu“ Cíl č. 5 „Efektivní a centrálně koordinované ICT veřejné správy“ Podporované oblasti kybernetické bezpečnosti: • činnosti v oblasti zabezpečení dat, jejich přenosu, ale i poskytování, • projekty v oblasti zvyšování bezpečnosti, interoperability a standardizace systémů a aplikací ve veřejné správě.
Cílové skupiny	Z realizace projektu budou plynout přínosy následujícím cílovým skupinám: - zaměstnanci ve veřejné správě (úředníci MěÚ Znojmo) - občané (občané spádové oblasti města Znojmo) - podnikatelské subjekty (podnikatelé spádové oblasti města)

Relevantní projekty a jejich vazba na projekt	Předkládaný projekt přímo nenavazuje na nějaký již realizovaný projekt obdobného charakteru. Město Znojmo průběžně obnovuje a modernizuje svoje IT vybavení včetně prvků zajišťujících kybernetickou bezpečnost, dosud však na proběhlé realizace nebylo využito žádného dotačního titulu. Z pohledu plánovaných projektů budou další aktivity města závislé na dotačních možnostech a pravidlech s tím spojených. V tuto chvíli není zpracován žádný konkrétnější projektový záměr v oblasti eGovernmentu.
Poskytovatel podpory	Ministerstvo vnitra ČR, Nad Štolou 936/3, Praha 7, 170 34 ID datové schránky 6bnaawp
Zdroje financování	NPO, vlastní zdroje žadatele
Pilíř	1. Digitální transformace
Název komponenty	1. 2 Digitální systémy veřejné správy
Reforma/Investice	Investice 5: Navýšení investic do kybernetické bezpečnosti
Identifikace výzvy	41 Kybernetická bezpečnost - obce
Název milníku/cíle	Informační systémy, jejichž kybernetická bezpečnost byla posílena v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti
Číslo milníku/cíle	Cíl (T248)
Termín splnění milníku/cíle	31.5.2026

1.3. Monitorovací indikátory

Název:	**Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému**
Typ indikátoru (společný/hlavní/interní):	Hlavní
Popis indikátoru:	Certifikát (akceptační protokol nebo podobný dokument) vydaný v souladu s národní legislativou kompetentním orgánem vlastnícím daný informační systém osvědčující zvýšení kybernetické bezpečnosti informačního systému v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
Měrná jednotka:	*Dokumenty*
Výchozí hodnota:	*0*
Datum výchozí hodnoty:	*1.9.2023*
Cílová hodnota indikátoru:	*1*
Datum cílové hodnoty:	*31.5.2026*
Způsob doložení:	*Dokument*
Frekvence:	*Průběžně*

Název:	**Seznam informačních systémů vybraných v souladu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti, jejichž kybernetická bezpečnost bude posílena**
Typ indikátoru (společný/hlavní/interní):	Hlavní

Popis indikátoru:	Dokument obsahující seznam informačních systémů vybraných v souladu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti, jejichž kybernetická bezpečnost bude posílena.
Měrná jednotka:	*Dokumenty*
Výchozí hodnota:	*0*
Datum výchozí hodnoty:	*1.9.2023*
Cílová hodnota indikátoru:	*1*
Datum cílové hodnoty:	*31.5.2026*
Způsob doložení:	*Dokument*
Frekvence:	*Průběžně*

Název:	**Dokument potvrzující úspěšné testování a ověření souladu s požadavky na kybernetickou bezpečnost**
Typ indikátoru (společný/hlavní/interní):	Hlavní
Popis indikátoru:	Certifikát (protokol nebo podobný dokument) podepsaný kompetentním orgánem vlastnící daný informační systém a dodavatelem potvrzující úspěšné a zdokumentované testování a ověření souladu s požadavky kybernetické bezpečnosti – tj. audit kybernetické bezpečnosti podle VKB v rozsahu plnění realizovaného v projektu.
Měrná jednotka:	*Dokumenty*
Výchozí hodnota:	*0*
Datum výchozí hodnoty:	*1.9.2023*
Cílová hodnota indikátoru:	*1*
Datum cílové hodnoty:	*31.5.2026*
Způsob doložení:	*Dokument*
Frekvence:	*Průběžně*

1.4. Rozpad projektu na hlavní produkty

I. Hlavní produkt	
ZÁKLADNÍ INFORMACE	
Název produktu:	**Posílené IS v rámci zabezpečení kyberbezpečnosti**
Počet posílených IS:	*17*
Názvy posílených IS:	• 8369 Scarabeus • 8297 Portál občana

	• 7227 Mapserver • 7226 Stavební úřad • 7223 Přestupky • 7221 Personalistika • 7138 YAMACO • 4933 MP Manager • 757 FLUXPAM5 • 684 Evidence myslivosti – EMY • 683 Evidence správních řízení – ESPI • 682 Ochrana ovzduší • 681 VITA • 613 HeleTax • 612 Evidence odpadů – EVI • 611 Editor vodoprávní evidence – eVPE • 497 GINIS
Předpokládané zahájení realizace produktu (dd. mm. rrrr):	1.11.2023
Předpokládané ukončení realizace produktu (dd. mm. rrrr):	31.5.2026
Celkové výdaje produktu bez DPH (Kč):	23 577 320 Kč
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor produkt navazuje:	Seznam informačních systémů vybraných v souladu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti, jejichž kybernetická bezpečnost bude posílena.
Popis produktu:	
Předmětem realizace celého projektu je modernizace a rozšíření stávajícího HW a SW vybavení městského úřadu ve Znojmě. Projekt bude mít kladný vliv na zvýšení efektivnosti a dynamičnosti poskytovaných služeb v rámci agendy úřadu. Dojde k doplnění informačního systému o nové dílčí subsystémy k vytvoření celistvé softwarové platformy pro zajištění komplexní kybernetické bezpečnosti úřadu. Realizace projektu bude mít přímý vliv na fungování 17 informačních systémů: • 8369 Scarabeus • 8297 Portál občana • 7227 Mapserver • 7226 Stavební úřad • 7223 Přestupky • 7221 Personalistika • 7138 YAMACO • 4933 MP Manager • 757 FLUXPAM5	

• 684 Evidence myslivosti – EMY • 683 Evidence správních řízení – ESPI • 682 Ochrana ovzduší • 681 VITA • 613 HeleTax • 612 Evidence odpadů – EVI • 611 Editor vodoprávní evidence – eVPE • 497 GINIS	
Způsob prokázání dokončení produktu:	**Dokument (seznam IS)**

II. Hlavní produkt	
ZÁKLADNÍ INFORMACE	
Název produktu:	**Zajištění finálního nezávislého auditu ověřujícího naplnění kybernetických požadavků**
Předpokládané zahájení realizace produktu (dd. mm. rrrr):	18.9.2025
Předpokládané ukončení realizace produktu (dd. mm. rrrr):	31.5.2026
Celkové výdaje produktu bez DPH (Kč):	230 000 Kč
Vazba na VZ:	3. Audit kybernetické bezpečnosti
Uveďte, na jaký monitorovací indikátor produkt navazuje:	Dokument potvrzující úspěšné testování a ověření souladu s požadavky na kybernetickou bezpečnost.
Popis produktu:	
Audit kybernetické bezpečnosti bude mít na konci realizace projektu za cíl posoudit a hodnotit úroveň bezpečnosti zavedených informačních technologií a kybernetických prostředí v organizaci. Cílem tohoto procesu bude ověřit, zda jsou implementovaná bezpečnostní opatření dostatečná k ochraně aktiv, dat a systémů před kybernetickými hrozbami. Audit kybernetické bezpečnosti bude proveden externím certifikovaným subjektem (nezávislým auditem nebo certifikačním orgánem).	
Způsob prokázání dokončení produktu:	**Dokument (výsledky auditu)**

III. Hlavní produkt	
ZÁKLADNÍ INFORMACE	
Název produktu:	**Administrativa projektu**
Předpokládané zahájení realizace produktu (dd. mm. rrrr):	1.9.2023
Předpokládané ukončení realizace produktu (dd. mm. rrrr):	16.8.2025
Celkové výdaje produktu bez DPH (Kč):	100 000 Kč

Vazba na VZ:	-
Uveďte, na jaký monitorovací indikátor produkt navazuje:	-
Popis produktu:	
Činnosti nepřímo související s projektem podle podmínek výzvy – administrativní náklady pořizované formou služby – zpracování žádosti o dotaci, organizace veřejné zakázky.	
Způsob prokázání dokončení produktu:	AKCEPTAČNÍ PROTOKOL

IV. Hlavní produkt	
ZÁKLADNÍ INFORMACE	
Název produktu:	**Ostatní aktivity a služby spojené s realizací projektu**
Předpokládané zahájení realizace produktu (dd. mm. rrrr):	17.8.2025
Předpokládané ukončení realizace produktu (dd. mm. rrrr):	31.5.2026
Celkové výdaje produktu bez DPH (Kč):	880 000 Kč
Vazba na VZ:	1. Analýza rizik
Uveďte, na jaký monitorovací indikátor produkt navazuje:	-
Popis produktu:	
Díky analýze rizik kyberbezpečnosti budou identifikovány, hodnoceny a řízeny potenciální hrozby a zranitelnosti informačních systémů města a celého kyberprostředí s cílem minimalizovat nebo eliminovat možné škody. Tato analýza je klíčovým prvkem efektivní kyberbezpečnostní strategie. Součástí projektu je také administrativní zajištění realizace projektu – pracovníci na DPP po dobu fyzické realizace projektu.	
Způsob prokázání dokončení produktu:	AKCEPTAČNÍ PROTOKOL

1.5. Rozpad hlavních produktů na podprodukty

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 1	
Název podproduktu:	**IS Scarabeus**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům.

	Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení.

	SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

***Podprodukty v rámci I. hlavního produktu* - Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 2	
Název podproduktu:	**IS Portál občana**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export),

	- změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů.

	Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 3	
Název podproduktu:	**IS Mapserver**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export),

	- změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů.

	Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 4	
Název podproduktu:	**IS Stavební úřad**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export),

	- změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů.

	Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 5	
Název podproduktu:	**IS Přestupky**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export),

	- změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů.

	Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 6	
Název podproduktu:	**IS Personalistika**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export),

	- změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů.

	Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

***Podprodukty v rámci I. hlavního produktu* - Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 7	
Název podproduktu:	**IS YAMACO**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export),

	- změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů.

	Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 8	
Název podproduktu:	**IS MP Manager**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export),

	- změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů.

	Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 9	
Název podproduktu:	**IS FLUXPAM5**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export),

	- změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů.

	Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 10	
Název podproduktu:	**IS Evidence myslivosti – EMY**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export),

	- změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů.

	Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.

	Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky.

	Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci I. hlavního produktu - **Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 11	
Název podproduktu:	**IS Evidence správních řízení – ESPI**
Stav podproduktu:	Realizován
Popis technických opatření, která budou posilovat IS:	**OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení).

	Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin.

	Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix).

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☐	☐	☐	☒	☐	☒	☒	☐	☐	☐

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.12.2024**
Celkové výdaje podproduktu bez DPH (Kč):	**36 141,65 KČ**
Vazba na VZ:	4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

***Podprodukty v rámci I. hlavního produktu* - Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 12	
Název podproduktu:	**IS Ochrana ovzduší**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců.

	Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce.

	Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu.

	Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově

	servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení:

	• 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

***Podprodukty v rámci I. hlavního produktu* - Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 13	
Název podproduktu:	**IS VITA**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace

	jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery,

	crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy.

	Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového

	centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28

	• 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

***Podprodukty v rámci I. hlavního produktu* - Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 14	
Název podproduktu:	**IS HeleTax**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude

	postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS.

	Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP).

	Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném

	prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště

	• 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

***Podprodukty v rámci I. hlavního produktu* - Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 15	
Název podproduktu:	**IS Evidence odpadů – EVI**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co

	nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning).

	Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa

	Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií.

	Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:											
§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

***Podprodukty v rámci I. hlavního produktu* - Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 16	
Název podproduktu:	**IS Editor vodoprávní evidence – eVPE**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita

	Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce. Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows.

	Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti. Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole.

	Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD. Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB.

	Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27

☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,65 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

***Podprodukty v rámci I. hlavního produktu* - Posílené IS v rámci zabezpečení kyberbezpečnosti**	
PODPRODUKT Č. 17	
Název podproduktu:	**IS GINIS**
Stav podproduktu:	Plánován
Popis technických opatření, která budou posilovat IS:	**NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT (NAPLNĚNÍ §19 A §20 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Organizace ve svém prostředí neprovozuje/provozuje certifikační autoritu a není/je tak aktuálně možné do jejího prostředí zavést dvou faktorovou autentizaci na základě PKI, jak nařizuje § 19 (3) vyhlášky č. 82/2018 Sb. Organizace proto chce zajistit zvýšení své kybernetické bezpečnosti a zároveň zabezpečit digitální ochranu svých zaměstnanců. Nejvhodnějším způsobem, je po interních diskuzích zavedení hybridních čipových karet pro hostování mimo jiné privátních klíčů a certifikátů. Tento autentizační nástroj bude přidělen každému zaměstnanci, aby byla zabezpečena dvou faktorová autentizace jejího držitele do PC a dalších systémů, jak hovoří §25 vyhlášky č. 82/2018 Sb. Cílem organizace je tedy zavedení hybridních čipových karet pro dvou faktorovou autentizaci. Tato autentizační metoda bude postavena na certifikátech vydávaných z doménového PKI. Spolu s tímto prostředkem zavézt nadstavbové aplikace, které co nejvíce zjednoduší a zautomatizují práci s těmito prostředky a certifikáty, tak jak je popsán požadovaný stav a funkcionality níže. Digitální identita Dodané řešení musí splnit veškeré požadavky organizace. Jedná se o scénáře, které personál vykonává každý den. Požadavky na zabezpečení procesů se liší podle toho, o jakého konkrétního zaměstnance jde – běžný uživatel nebo správce.

	Autentizační prostředek –čipová karty zabezpečí všechny požadované operace, které uživatel denně vykonává, a to: - více faktorové ověření zaměstnance organizace do informačních systémů a potřebných zařízení, - autentizace zaměstnance při přístupu do vzdálené plochy nebo terminálových služeb, - vizuální identifikace držitele Autentizační prostředek bude v souladu s § 12 vyhlášky č. 82/2018 Sb. O vydávání a správu autentizačních prostředků se budou starat odpovědné osoby určené organizací. Životní cyklus autentizačních prostředků a certifikátů je složen z několika kroků, a proto je požadováno usnadnění a zjednodušení jejich správy odpovědným osobám, tak i koncovým uživatelům. Řešení bude zahrnovat SW podporu, zejména: - manuální správa dat čipové karty (import a export), - změna a odblokování bezpečnostních kódů čipové karty uživatelem. **OCHRANA KONCOVÝCH STANIC SERVERŮ PŘED ŠKODLIVÝM KÓDEM (NAPLNĚNÍ §21, §23 A §24 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím. Součástí dodaného řešení bude také jeho implementace v prostředí MěÚ Znojmo a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 5 let. Antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení bude od jednoho výrobce. Ochrana pracovních stanic a serverů Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. Ochrana před exploitací instalovaných aplikací a OS. Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning). Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce). Kontrola paměti a detekce Fileless Threats ve Windows. Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti.

	Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE). Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook. Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu. Ochrana a správa mobilních zařízení typu SmartPhone/tablet Podpora pro OS Android a iOS. Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení). Detekce root/jailbreak zařízení. SMS/MMS AntiSpam a filtr nevyžádaných hovorů. Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace). Zabezpečení on-line komunikace (firewall). Zašifrování obsahu mobilního zařízení. Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií. Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů. Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět. Optimalizovaná ochrana pro virtuální prostředí Agentless antimalware zabezpečení pro VMware. Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix. Podpora AWS a MS Azure veřejného/privátního cloudu. Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy. Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací. Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP). Kontrola integrity systémových souborů, logů a kritických aplikací. Centrální správa Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole. Podpora Windows Server 2019 a výše, MS SQL Server 2019 (Express) a výše, MySQL 5.5 a výše. Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD.

	Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet. Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku. Instalace endpoint aplikace na serverech bez nutnosti restartu. Zabezpečené spojení mezi serverem centrální správy a endpoint agenty. Podpora Active Directory a IPv6. Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie. Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě. Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. Podpora virtuálního prostředí (VMware, Hyper-V, Citrix). **NÁSTROJ PRO BEZPEČNÉ UKLÁDÁNÍ DAT A INFORMACÍ (NAPLNĚNÍ §18 A §27 VYHLÁŠKY O KYBERBEZPEČNOSTI)** Projekt počítá s modernizací stávající HW infrastruktury MěÚ Znojmo. Jako podklad pro návrh specifikace projektu bylo provedeno měření pomocí LiveOptic. Z tohoto měření vyplynul závěr potřeby navýšení výkonu za účelem vysoké dostupnosti – režimu HA na Datovém centru 1, kde nedostačují výkonově servery a disková pole pro „tento“ režim vysoké dostupnosti. Následně není nyní žádná fyzicky oddělená lokalita v případě poruchy Datového centra 1. Pořízením technologie do Datového centra 2 se zajistí provoz při nefunkčnosti zásadních komponent a jiných technických problémech na Datovém centru 1. Z pohledu bezpečnosti je nutné řešit zálohy nejlépe v geograficky odděleném prostředí, což bylo zvoleno Datové centrum 3, kde budou uloženy zálohy (Backup) z provozních technologií. Trezorové řešení pro ukládání dat – izolované, z interní sítě / internetu technicky nedostupné, řešení pro uložení neměnných záloh o minimálním datovém prostoru 24 TB. Backup – zálohování bude řešeno SW licencí pro tvorbu provozní zálohy a zároveň přípravu zálohy pro izolované / trezorové uložení. V prvním kroku, po vytvoření prvních plných záloh do backup serveru (Server C), se budou na bázi denních inkrementů

	připisovat do backup serveru. Následně budou zálohy kontrolovány, ukládány a šifrovány – uzamčeny do trezorového řešení. Operace pro bezpečnou / trezorovou zálohu budou používány inkrementy záloh obdobně jako u provozního backupu. Trezorová záloha musí sloužit jako instance poslední záchrany např. před Ransomware a jinými podobnými útoky a kryptoviry. Propojení lokalit – lokality vzájemně propojené optickými vlákny o minimální propustnosti 25Gb/s (záležitost koncových bodů GBIC modulů switchů). Otická vlákna k jednotlivým přípojným bodům mezi lokalitami jsou již v provozu, nejsou tudíž předmětem / součástí zakázky. Režim HA – na Datovém centru 1 budou umístěny 2 servery o identické konfiguraci. Při výpadku jednoho ze serverů, si převezme druhý server virtuální servery z prvního na úrovni virtualizační platformy vč. možnosti omezení výkonu virt. serverů pro bezproblémový chod na tomto serveru do doby odstranění závady / poruchy. Druhá záložní lokalita – na Datové centrum 2 bude umístěn jeden server, který výkonově (počtem jader CPU, RAM, …) dokáže převzít v disaster recovery plánu kompletně všechny virtuální stroje z Datového centra 1. Replikace diskových polí – synchronní replikace diskových polí mezi Datovými centry 1 a 2 – nastavení na úrovni výrobce diskových polí – pokud je třeba jakákoliv licence výrobce, je nutné zahrnout do nabídky. Předpokládá se pořízení následujícího vybavení: • 6 ks - Core/Server Switch, 24 x 25GbE SFP28, 4 x 100GbE, QSFP28 • 1 ks - Access Switch, 28 x 10 Gbase-T, 2 x QSFP28 • 4 ks - SAN Switch (24 x 32Gb SFP28) • 4 ks - virtualizační server • 2 ks - sdílené diskové úložiště • 1 ks - komplexní zálohovací systém – bezpečné úložiště, izolovaný datový trezor s funkcí ochrany proti zašifrování dat

Vazba na § vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti *(zaškrtnout, ke kterým § se technická opatření vztahují)*:

§ 3	§ 16	§ 18	§ 19	§ 20	§ 21	§ 22	§ 23	§ 24	§ 25	§ 26	§ 27
☐	☐	☒	☒	☒	☒	☐	☒	☒	☐	☐	☒

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1.11.2023 – 31.5.2026**

Celkové výdaje podproduktu bez DPH (Kč):	**1 471 323,6 KČ**
Vazba na VZ:	2. Zajištění kybernetické bezpečnosti MěÚ Znojmo 4. Dodávka antimalware zabezpečení
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	Dokument potvrzující zvýšení kybernetické bezpečnosti informačního systému.
Způsob prokázání dokončení podproduktu:	**Akceptační protokol**

Podprodukty v rámci III. hlavního produktu – Administrace projektu	
PODPRODUKT Č. 1	
Název podproduktu:	**ŽÁDOST O DOTACI VČETNĚ VŠECH POVINNÝCH PŘÍLOH**
Stav podproduktu:	Ukončen
Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**1. 9. 2023 – 31. 12. 2023**
Celkové výdaje podproduktu bez DPH (Kč):	**70 000 KČ**
Vazba na VZ:	**-**
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	**-**
Popis podproduktu:	
Administrativa spojená s přípravou a podáním žádosti o podporu. Součástí poskytnuté služby je zpracování žádosti o podporu v systému ISKP14+, zpracování projektové žádosti, zajištění souhlasného stanoviska OHA.	
Vazba na jiné podprodukty:	
Zpracování žádosti o podporu a získání finančních prostředků na zajištění realizace má zásadní vliv na všechny ostatní realizované aktivity (podprodukty) projektu.	
Způsob prokázání dokončení podproduktu:	AKCEPTAČNÍ PROTOKOL

Podprodukty v rámci III. hlavního produktu - Administrace projektu	
PODPRODUKT Č. 2	
Název podproduktu:	**ORGANIZACE VEŘEJNÉ ZAKÁZKY**
Stav podproduktu:	Plánován

Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**15.5.2025 – 16.8.2025**
Celkové výdaje podproduktu bez DPH (Kč):	**30 000 KČ**
Vazba na VZ:	**-**
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	**-**
Popis podproduktu:	
Zajištění administrace otevřeného nadlimitního řízení na hlavní součásti realizace projektu – veřejná zakázka s názvem - Zajištění kybernetické bezpečnosti Znojmo.	
Vazba na jiné podprodukty:	
Zajištění administrace veřejné zakázky bude mít zásadní vliv na podprodukty, které mají být v rámci zakázky „Zajištění kybernetické bezpečnosti MěÚ Znojmo“ realizovány.	
Způsob prokázání dokončení podproduktu:	AKCEPTAČNÍ PROTOKOL

Podprodukty v rámci IV. hlavního produktu – Ostatní aktivity a služby spojené s realizací projektu	
PODPRODUKT Č. 1	
Název podproduktu:	**ANALÝZA RIZIK**
Stav podproduktu:	Plánován
Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**17.8.2025 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**460 000 KČ**
Vazba na VZ:	**1. Analýza rizik**
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	**-**
Popis podproduktu:	
Díky analýze rizik kyberbezpečnosti budou identifikovány, hodnoceny a řízeny potenciální hrozby a zranitelnosti informačních systémů města a celého kyberprostředí s cílem minimalizovat nebo eliminovat možné škody. Tato analýza je klíčovým prvkem efektivní kyberbezpečnostní strategie. Dokumentace bude pravidelně aktualizována. Opatřením dojde k naplnění § 3 vyhlášky o kybernetické bezpečnosti.	

Vazba na jiné podprodukty:	
Analýza rizik se bude prolínat všemi dalšími aktivitami realizovanými v rámci tohoto projektu – hodnocení realizovaných aktivit.	
Způsob prokázání dokončení podproduktu:	AKCEPTAČNÍ PROTOKOL

Podprodukty v rámci IV. hlavního produktu – Ostatní aktivity a služby spojené s realizací projektu	
PODPRODUKT Č. 2	
Název podproduktu:	**MZDOVÉ NÁKLADY**
Stav podproduktu:	Plánován
Předpokládané období realizace podproduktu od – do (dd. mm. rrrr):	**17.8.2025 – 31.5.2026**
Celkové výdaje podproduktu bez DPH (Kč):	**420 000 KČ**
Vazba na VZ:	**-**
Uveďte, na jaký monitorovací indikátor podprodukt navazuje:	**-**
Popis podproduktu:	
Zajištění kapacity interních pracovníků při přípravě a realizaci projektu.	
Vazba na jiné podprodukty:	
Zajištění administrativy a dohledu ze strany pracovníků bude mít přímý vliv na realizaci veřejné zakázky na dodávku jednotlivých komponent projektu a na samotné dodání a implementaci.	
Způsob prokázání dokončení podproduktu:	AKCEPTAČNÍ PROTOKOL

2. Rizika, omezení a předpoklady úspěšnosti projektu

2.1. Rizika projektu

Č.	Riziko	Způsob snížení dopadu/eliminace rizika	Ohodnocení rizika (1 – 3)
1	Dodatečné změny požadavků investora	Předkládaný projekt byl dlouho zvažován a upravován před jeho předložením v této podobě. Navržené řešení vychází z analýzy stávajícího stavu. Předkládaná podoba je finální a je ve všech ohledech vyhovující a dlouhodobě udržitelná. Z tohoto důvodu je riziko zanedbatelné.	1
2	Výběr nekvalitního dodavatele	Zárukou vhodného výběru dodavatele by mělo být vhodné nastavení podmínek výběrového řízení a ověření poskytnutých referencí. Případné problémy jako nekvalitně odvedená práce, neplnění termínů, špatná komunikace atd. budou ošetřeny ve smlouvě s daným dodavatelem a budou finančně postihovány. V případě velice závažných problémů bude smlouvy rozvázána a bude vybrán jiný dodavatel.	2
3	Nedodržené termínu realizace	Harmonogram byl zpracován odborníky se zkušenostmi v oboru, vychází z odborného odhadu projektanta a byla započítána také dostatečná časová rezerva pro případ neočekávaných komplikací. Nedodržení harmonogramu je tedy prakticky vyloučeno.	2
4	Neobdržení dotace	Pro eliminaci rizika byla provedena pečlivá projektová příprava, spojená s konzultováním záměru s poradenskou společností a řídícím orgánem. Veškeré podmínky stanovené výzvou předkládaný projekt splňuje a je tedy pouze otázkou veřejné soutěže, zda bude či nikoliv tento projekt úspěšný. V případě neudělení dotace by byl projekt těžko realizován a také by tento fakt měl vliv na další plánované projekty žadatele.	2
5	Nedostatek finančních prostředků na předfinancování a v průběhu realizace projektu, neočekávané zvýšení cen v průběhu realizace	Žadatel má podrobný finanční plán na realizační i provozní fázi projektu a má dostatečné finanční zajištění, aby ho pokryl. Rozpočet byl sestaven s nejvyšší péčí podle současných tržních cen a odpovídá reálným možnostem žadatele předfinancovat a také spolufinancovat projektové výdaje. Žadatel má i rezervy pro pokrytí případných vícenákladů a nečekaných výdajů.	2
6	Nedostatek finančních prostředků v provozní fázi projektu	Žadatel má vypracován finanční plán, díky kterému má dobrou představu o nákladech spojených s provozem sociální služby. Případné neočekávané náklady je žadatel schopen pokrýt z vlastních zdrojů, má pro ně v rozpočtu vyhrazeny prostředky a má i dostatečnou rezervu pro větší výdaje.	1

2.2. Omezení projektu

Organizační a technologická omezení	Organizační a technologická omezení se při realizaci projektu neočekávají. Tým, který se na přípravě a realizaci projektu podílí, byl sestaven z odborníků, kteří mají bohaté zkušenosti s danou oblastí a odbornou způsobilost. Projektový tým byl zainteresován po celou dobu přípravy projektu a je s projektem dostatečně obeznámen. Pokud by bylo potřeba v průběhu realizace některé členy týmu zastoupit, žadatel má dostatečné personální zajištění, aby našel adekvátní náhradu.
Legislativní omezení	Žadatel je dobře obeznámen s podmínkami právních norem ČR a EU, nejasnosti byly konzultovány s právním oddělením externí poradenské agentury, která bude všechny kroky žadatele při realizaci i udržitelnosti projektu kontrolovat, aby nedošlo k porušení právních norem.
Bezpečnostní omezení	Realizace projektu není omezena žádnými bezpečnostní omezeními.

3. Připravenost projektu k realizaci

Popis, jak je projekt připraven k realizaci:
Všechny součásti projektu jsou připraveny k zahájení realizace a v případě přiznání dotace bude moci být zahájena veřejná zakázka na dodavatele celého bezpečnostního řešení.

4. Udržitelnost projektu

Popis udržitelnosti:
Udržitelnost projektu z hlediska provozního bude zajištěna dodavatelsko-odběratelskou smlouvou ze strany města Znojmo a dodavatelem vybavení. Při pořizování nových prvků kybernetické bezpečnosti budou dodrženy všechny podmínky pro zadávání veřejných zakázek dle pravidel řídícího orgánu a dle podmínek pro zadávání veřejných zakázek. Veškeré vybavení pořízené v rámci projektu zůstane v majetku žadatele po celou dobu udržitelnosti projektu. Po finanční stránce projektu v době udržitelnosti budou veškeré náklady spojené s provozem a údržbou hrazeny z rozpočtu žadatele, tedy města Znojmo. V době udržitelnosti nejsou uvažovány žádné další náklady nad rámec provozních nákladů. Aktuální organizační připravenost projektu je zajišťována projektovým týmem, který se angažuje v přípravě projektové žádosti a všech potřebných podkladů pro předložení projektu. Tyto osoby celkový organizační proces projektu plně koordinačně zabezpečují. Zodpovědnost za celý projekt nese hlavní manažer projektu, který řídí spolupráci s externími společnostmi. Do aktuální přípravné fáze spadá primárně zpracování této studie proveditelnosti a žádosti o dotaci, které jsou realizovány externí poradenskou agenturou. Projektovým týmem bude v jednotlivých fázích projektu zejména sledováno a kontrolováno postupné naplňování cílů projektu a průběh jeho časového harmonogramu a budou vyhodnocována a eliminována případná rizika projektu. Nakupované služby v rámci projektu budou využity výhradně pro realizaci projektu a pro účely využití vymezené projektem. Projekt je zpracován na základě požadavků výzvy a jeho dosavadní zpracování obsahuje všechny potřebné dokumenty pro podání projektové žádosti. Žadatel zodpovídá za předkládaný projekt po dobu udržitelnosti, ve všech aspektech projektu.

5. Projektový tým

Role
Statutární zástupce žadatele - Mgr. František Koudela, starosta
Projektový manažer - Ing. et Ing. Růžena Salvetová – administrátor dotace
Odborný gestor - Ing. Lubomír Otepka, vedoucí oddělení informatiky
Technický gestor - Ing. Lubomír Otepka, vedoucí oddělení informatiky

Je ustaven projektový tým v době podání žádosti o podporu?	ANO

6. Veřejné zakázky projektu

Číslo VZ	Název VZ	Způsob zadání VZ / Druh VZ	Předpokládaná/ skutečná hodnota VZ	Předpokládané / skutečné datum zahájení (dd. mm. rrrr)	Předpokládané / skutečné datum ukončení (dd. mm. rrrr)
1	Analýza rizik	Veřejná zakázka malého rozsahu	460 000 Kč bez DPH	1.8.2025	30.9.2025
2	Zajištění kybernetické bezpečnosti MěÚ Znojmo	Otevřené nadlimitní řízení	22 929 912 Kč bez DPH	1.8.2025	30.9.2025
3	Audit kybernetické bezpečnosti	Veřejná zakázka malého rozsahu	230 000 Kč bez DPH	1.9.2025	31.10.2025
4	Dodávka antimalware zabezpečení	Zjednodušené podlimitní řízení	647 408 Kč bez DPH	13.11.2023	7.12.2023

7. Horizontální principy

Typ horizontálního principu	Rovné příležitosti a nediskriminace
Vliv projektu na horizontální princip	Neutrální k horizontálnímu principu
Popis a zdůvodnění vlivu projektu na horizontální princip (v případě pozitivního nebo negativního vlivu)	

Typ horizontálního principu	Udržitelný rozvoj
Vliv projektu na horizontální princip	Neutrální k horizontálnímu principu

Typ horizontálního principu	Rovné příležitosti mužů a žen

Vliv projektu na horizontální princip	Neutrální k horizontálnímu principu
Popis a zdůvodnění vlivu projektu na horizontální princip (v případě pozitivního nebo negativního vlivu)	

8. Další údaje

Další údaje	

9. Schvalovací doložka

Podpis předkladatele (ředitele projektu)	Ing. et Ing. Růžena Salvetová (na základě plné moci)
Datum podání žádosti	

Ing. Růžena Salvetová
Digitálně podepsal Ing. Růžena Salvetová
Datum: 2025.07.02 13:37:29 +02'00'

10. Přílohy

Seznam povinných příloh je definován výzvou (kapitola 7.1 Povinné přílohy)

Seznam příloh předložených s žádostí o finanční podporu:
Projektová žádost podepsaná (pdf.)
Projektová žádost nepodepsaná (word)
Stanovisko OHA
Jmenovací dekret statutárního zástupce organizace
Plná moc od statutárního zástupce organizace pro ředitele projektu
Studie proveditelnosti / Nerelevantní příloha
Harmonogram
Čestné prohlášení
Interní akt příjemce pro zadávání veřejných zakázek
Čestné prohlášení ke střetu zájmů
Pověřovací akt k poskytování SOHZ / Nerelevantní příloha
Čestné prohlášení žadatele k Souhlasnému stanovisku OHA
Analýza výchozího stavu
Souhlasné stanovisko zřizovatele s realizací projektu / Nerelevantní příloha
Tabulka vymezení činností/služeb, které budou podpořeny v rámci finanční podpory
Čestné prohlášení žadatele o finanční podporu malého rozsahu - de minimis / Nerelevantní příloha
Doklad o bankovním účtu