Příloha č. 1 Smlouvy Technická specifikace

Technická specifikace

"Nástroj pro analýzu rizik a řízení KB v ONN a.s."

Předmětem je pořízení SW nástroje určeného pro zavedení a následné správě a řízení ISMS dle ISO/IEC 27001:2014 v kontextu ZoKB a VoKB včetně technické a legislativní podpory v délce 48 měsíců.

Zkratky:
AKB – Architekt kybernetické bezpečnosti
ISMS - Information Security Management Systém – Systém řízení bezpečnosti informací
ONN – Oblastní nemocnice Náchod
MKB – Manažer kybernetické bezpečnosti
NIS 2 - Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v EU a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148
NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost
ZoKB - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
VoKB - Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat

Zadavatel si vyhrazuje právo odmítnout navrhované řešení, pokud nebude v souladu s doporučeními a varováními vydanými Národním úřadem pro kybernetickou a informační bezpečnost, zejména ve vztahu k rizikovým dodavatelům.
Zadavatel si vyhrazuje právo si vyžádat funkční vzorek pro otestování systému na základě písemné výzvy, a to ve fázi posouzení splnění podmínek účasti v zadávacím řízení.

Položka č.	Popis minimáních funcionalit systému		
1	**SW nástroj musí minimálně splňovat:**	**Splňuje (ANO/NE)**	**Hodnota parametru účastníka** (odkaz na číslo stránky v produktovém listu/technické specifikaci apod.)
1.1.	evidence a hodnocení aktiv zadavatele (kupujícího) dle metodiky definované VoKB	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik str. 1-3
1.2.	prezentace datových sad - pohled na aktiva, zhodnocení závislostí mezi aktivy, hodnocení aktiv a rizik	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Hodnocení aktiv"
1.3.	metodické vedení bezpečnostní role při identifikaci - hodnocení aktiv a řízení rizik	ano	SW podporuje nastevení hodonocení aktiv a hodnocení rizik podle interní metodiky klienta a uživatele (jednotlivé bezpečnostní role) jsou potom "vedené " při vyplnovaní karet aktiv nastavenými parametry a číselníky. Zároveň sw umožnije spustit i "wizard" při analýze rizik.
1.4.	hodnocení rizik prostřednictvím automatizovaného výpučtu hodnoty rizika	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Hodnocení rizika"
1.5.	vytvoření Prohlášení o aplikovatelnosti dle definice VoKB	ano	Pro vytvoření Prohlášení o aplikovatelnosti se používá modul standarty/kvalita, ve kterém je uživatelsky editovatelný registr externích požadavků (vazeb na jednotlivé požadavky VKB). Zde se definuje míra relevatnosti a způsob plnění těchto požadavků. A to jak textovou formou, tak i interpretací datových vazeb na jiné obejty (procesy, dokumenty, indikátory,...) V rámci implementace ptom nastavujeme tiskový výstup do pdf.
1.6.	vytvoření a evidence Plánu zvládání rizik dle definice VoKB	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Rozhodnutí o zvládání jednotlivých rizik a návrh opatření"
1.7.	automatické logy změnv rámci životního cyklu aktiv a rizik	ano	Přímo v kartě aktiva je možné zobrazit audit změn, který lze při implementaci konfigurovat. Karta rizika je navíc plně verzována.
2	**Požadavky na aktiva:**	**Splňuje (ANO/NE)**	**Hodnota parametru účastníka** (odkaz na číslo stránky v produktovém listu/technické specifikaci apod.)
2.1.	evidence aktiv, jež jsou předdefinovaná s rozdělením na primární a podpůrná s možností editace a vkládání dalších položek	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Identifikace aktiv, naplnění seznamu zdrojů (aktiv) a stanovení vlastníků aktiv"
2.2.	evidence atributů aktiv (předdefinované i vlastní) včetně generování karet aktiv	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Identifikace aktiv, naplnění seznamu zdrojů (aktiv) a stanovení vlastníků aktiv"
2.3.	import a export aktiv (např. xls apod.)	ano	Tabulkové přehledy v celé aplikaci lze exortovat do xls. Pro importy do DB (i exorty) lze používat standartní MS Powershell.
2.4.	vytvoření a přiřazení garantů k aktivům, každý garant aktiv má přístup ke svým (přiřazeným) aktivům	ano	U všech datových objektů kde je vazba na vlastníka, garanta, ověřovatele, správce se tyto objety automaticky zobrzují přihlášeným osobám v osobní stránce. (Rizka, Aktiva, Dokumenty, Procesy, Opatření,..)
2.5.	definice vlastních garantů atributů aktiv	ano	i všech dalších objektů, viz předchozí komentář.
2.6.	definice vlastní šablony aktiv a sady vlastních atributů aktiv	ano	definice vlastní šablony aktiv a sady vlastních atributů aktiv proběhne v rámci implementace systému
2.7.	doplnění textového popisu aktiva - možnost minimálně základního formát	ano	Editovatelný popis s formátvacím nástrojem je u všech standartních objektů /Proces, Dokument, Riziko, Aktivum, Hrozba, Zranitelnost,…)
2.8.	tvorba vazeb mezi aktivy - převedení vazeb aktiv do grafické podoby s možností filtrování v grafickém zobrazení vazeb aktiv včetně grafické úpravy polohy aktiv	ano	Vazby mezi aktivy se výtvářejí přímo v kartě aktiva kde lze zároveň zobrazovat hodnoty hodnocení souvisejích aktiv. V připravované verzi (předpokládané na začátek srpna 2024) bude i možnost zobrazovat vazby mezi aktivy a riziky v garafické komponentě (stejná jako je nyní pro modelování procesů)
2.9.	hodnocení aktiv a rizik	ano	Hodnotit aktiva lze v kontextu dopadové matice (dle metodiky NUKIB) kde lze předdefinovat hodocení i v jednotlivých oblastech dopadu.
2.10.	definice vlastní stupnice či její části pro hodnocení aktiv včetně hodnocení a kategorizace rizik	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Naplnění číselníků řízení rizik pro rizika pokročilá a zdroje/aktiva"
3	**Řízení rizik:**	**Splňuje (ANO/NE)**	**Hodnota parametru účastníka** (odkaz na číslo stránky v produktovém listu/technické specifikaci apod.)
3.1.	vytvoření a správa katalogu a karet rizik	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Vyplnění katalogu rizika a provedení analýzy rizik"
3.2.	vytvoření a správa registru hrozeb a zranitelností	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Naplnění číselníků řízení rizik pro rizika pokročilá a zdroje/aktiva"

3.3.	vytvoření a správa registru primárních a podpůrných aktiv, včetně jejich ho	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Identifikace aktiv, naplnění seznamu zdrojů (aktiv) a stanovení vlastníků aktiv" a kapitola "Hodnocení aktiv"
3.4.	vytvoření a správa podpůrných evidencí	ano	Definice podpůrných evidencí proběhne v rámci implementace systému
3.5.	definice a evidence opatření na úrovni každého aktiva, hrozby zranitelnosti, rizika s jednoznačnou identifikací zadavatele, řešitele a termínu plnění	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Rozhodnutí o zvládání jednotlivých rizik a návrh opatření"
3.6.	uživatelská tvorba vazeb mezi relevantními datovými entitami v systému	ano	Dokument: 00.01 - Základní ovládání systému, obr. "Obrázek 3 Základní zobrazení a ovládací tlačítka tabulek", tlačítko sponky připojí existující datovou entitu formou vazby
3.7.	definice správců aktiv, běžnýchuživatelů a jejich zapojení do správy rizik	ano	viz komentář ke 2.4. U aktiv lze navíc evidovat i jednotlivé uživatele. A všem uživatelem lze u všech datových objetů založit úkol.
3.8.	kontrola kozinstence modelu řízení rizik	ano	Pokud jsou v systému zadány vazby mezi datovými entitami a je potřeba zrušit nebo přidat vazby, systém vyzve uživatele k vypořádání všech existujích vazeb tak, aby byla ochráněna konzistence definovaného modelu
3.9.	uživatelsky definované číselníky pro nastavení metodiky řízení rizik (hodnoty výpočtu)	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Naplnění číselníků řízení rizik pro rizika pokročilá a zdroje/aktiva"
3.10.	tvorba a správa Plánu zvládání rizik	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Rozhodnutí o zvládání jednotlivých rizik a návrh opatření" - Plán zvládaní je souhrn všech opatření k rizikům, generuje se v přehledech
3.11.	podpora "hlášení" bezpečnostního incidentu nebo bezpečnostní idálosti ze strany bežných uživatelů s podporou workflow reakce zaměstnanců zadavatele na událost či incident s jednoznačným identifikátorem času a jména uživatele s povinností zaznamenat veškerou činnost spojenou se zvládáním bezpečnostních událostí/incidentů např. pro forenzní účely. Cílem je zaznamenání workflow "kdo, kdy co" učinil s nemožností další manipulace se záznamem po jeho uložení.	ano	Evidencie incidentů je realizována v modulu ServiceDesk. Požadované workflow bude nastaveno v rámci implementace.
3.12.	stanovení opatření k řešení rizik a jejich přiřazení konkrétním pracovním pozicím	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, obrázek "Obrázek 13 Karta opatření k riziku" a "Obrázek 7 Založení nového rizika z karty aktiva" Navíc lze jako optření stanovit i proces, dokument, který definuje "pravidlo" - opaření.
3.13.	kontrola plnění opatření s možností emailové notifikace	ano	Formou kontroly stavu úkolů na kartě aktiva, nebo v rámci modulu Úkoly s emailovou notifikací
3.14.	provádění auditů a kontrol	ano	V akrtách datových obejt lze přímo vytvářet záznamy o kontrolách a auditech s navazující možností definovat i opatření pokud je nějaký kontrolní nález.
Další požadavky:		**Splňuje (ANO/NE)**	**Hodnota parametru účastníka** (odkaz na číslo stránky v produktovém listu/technické specifikaci apod.)
4	**Definice hrozeb a zranitelností**	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Naplnění číselníků řízení rizik pro rizika pokročilá a zdroje/aktiva"
5	**Definici opatření pro snížení rizik**	ano	Dokument: 04.02 - Návod Pokročilé řízení rizik, kapitola "Rozhodnutí o zvládání jednotlivých rizik a návrh opatření"
6	**Reporty, vizualizace dashboardů nebo grafik k zobrazení zvolených výstupů**	ano	Dokument: 00.01 - Základní ovládání systému, obr. "Obrázek 1 Pohled na úvodní obrazovku" a Dokument: 03.02 - Návod Řízení výkonnosti kapitola "1.2 Obsah modulu Výkonnost"
7	**Řízení zdrojů zadavatele - např. aktiva, SW, HW, zdravotnická technika apod.**	ano	Evidencie a řízení zdrojů(aktiv) je realizována v modulu Řízení zdrojů. Součástí karet zdrojů je evidence a plánování údržby, revizí včetně možnosti vykazování časů nebo nákladů.
8	**Procesní řízení**	ano	Dokument: 08.01 - Modelování v ATTIS6
9	**Hodnocení přijatých opatření v minimálně tomto rozsahu:**	ano	Výkonnost"
	vyhodnocování plnění opatření včetně grafické vizualizace výsledků (nepř. ve formě "semaforů" apod.) pro manažerské shrnutí	ano	Dokument 03.02 - Návod Řízení výkonnosti
	vložení a editace různých komentářů a poznámek k opatřením.	ano	U všech datoavých objetů lze v kláda komentáře nebo poznámky.
10	**Řízená bezpečnostní dokumentace v minimálně tomto rozsahu:**	ano	Dokument: 02.02 - Pokročilé řízení dokumentů
	strukturované uspořádání dokumentů s možností rozčlenění do slože	ano	Domenty lze zařovat do složek a uspořádavat v rámci stromové struktury. Lze takto členit jak složky tak i jen dokumenty. (dokument má vnořené dalších N podokumentů)
	evidování verzí dokumentů,	ano	Dokument: 02.02 - Pokročilé řízení dokumentů
	hlídání termínů revizí dokumentů s množností emailové notifikace,	ano	Dokument: 02.02 - Pokročilé řízení dokumentů
	vytváření vazeb dokumentů k procesům zadavatele, rizikům apod.	ano	Dokument: 02.02 - Pokročilé řízení dokumentů
11	**Definice organizační struktury zadavatele - v minimálním rozsahu:**	ano	Dokument: 01.02.D1 - Stručný návod ke správě organizační struktury_modul ORG
	vytvoření dymanické organizační struktury pro zvládání bezpečnostních indicentů a událostí, včetně definování a vytvoření dočasné organizační struktury/jendotky.	ano	Dokument: 01.02.D1 - Stručný návod ke správě organizační struktury_modul ORG
	Podpora synchronizace číselníku oragnaizační struktury vůču stávajícímu IS zadavatele.	ano	sw disponije Web API pro jakékoli synchronizace
12	**Řízení dodavatelů, smluv a objednávek - v minimálním rozsahu:**	ano	Problematika je řešena v modulu Smlouvy a Adresář
	evidence dodavatelů s množností rozlišení významných dodavatelů,	ano	V rámci impemlementace nastavujeme kategorie a třídění dodavatelů (společnosti a kontaty)
	hodnocení dodavatelů dle VoKB,	ano	Lez hodnotit (klasifikovat dodavtele přímo v kartě společnsot nebo vytvořit struturovaný model pro pravidelné hodnocení dle definované hodnotící škály.
	řízení životního cyklu smluv.	ano	V rámci implementaci lze nastavit jednotlivé fáze cyklu nebo celé schvalovací a připomínkovací wf.
Požadavky na SW nástroj jako celek:		**Splňuje (ANO/NE)**	**Hodnota parametru účastníka** (odkaz na číslo stránky v produktovém listu/technické specifikaci apod.)
13	Nastavení různých přístupů pro jednotlivé bezpečnostní role, a to v rozsahu: Správce, Manažer KB, Garant/Vlastník aktiva, Administrátor) s možností vytváření vlastních rolí a s možností vytvoření testovacího přístupu, jež bude sloužit na testování a zaškolení nových uživatelů.	ano	Dokument: 01.02 - Návod - modul lidské zdroje , kapitola "3.3 Práce s procesními rolemi"

14	Definice přístupů pomocí skupin uživatelů	ano	Dokument: 01.02 - Návod - modul lidské zdroje , kapitola "3.3 Práce s procesními rolemi"
15	Práce více uživatelů souběžně min. 15	ano	V rámci dodávky poskytneme odpovídající počet licencí pro práci min. 15 souběžně pracujících uživatelů
16	Provedení GAP analýzy požadavků definovaných ZoKB, VoKB, ISO27001 - Prohlášení o aplikovatelnosti	ano	Pro Gap analýze se automaticky generuje přehled Aplikace standardů, který je součástí modulu Kvalita/Standardy
17	Vytvoření a editace bezpečnostních rolí a upravovat bezpečnostní organizační strukturu. Evidenci osob lze vytvořit manuálně i importem/synchronizací například z Microsoft Active Directory	ano	V rámci nastavení v aplikaci Synchronizaci s AD nastavejme v rámci implementace
18	Autentizace pomocí Active Directory (AD)/LDAP, vícefaktorová autentiuace či podpora Singl Sing On vůči OS Windows (SSO). Řízení oprávnění přes AD, pomocí doménových skupin. Řízení uživatelských	ano	AD. V připravované verzi jse možná autentizace prostřednictvím MS účtu s vícefaktorovou autentizací.
19	Řízení činností výboru pro kybernetickou bezpečnost od evidenci stanov a jednacího řádu, naplánování jednání, evidenci zápisů, evidenci úkolů a jejich plnění apod.	ano	V systému ATTIS evideujeme dokumenty(stanovy, řády, směrnice, vyhlášky apod.) v modulu Řízená dokumentace a plánování a realizaci úkolů(např.opatření), porady v modulu Úkoly, pro potřeby zakázky je poskutnut odpovídající počet licencí k daným modulům
20	Řízení činností garantů aktiv včetně evidence požadavků na změny jejich aktiv pomocí role MKB.	ano	Formou úkolů na kartě aktiva, nebo v rámci modulu Úkoly s emailovou notifikací
21	Řízení jednání a kontrolování plnění úkolů MKB/AKB.	ano	Formou úkolů a zápisů z porad evidovaných v systému nebo v rámci modulu Úkoly s emailovou notifikací
Požadavky na SW nástroj jako celek:		**Splňuje (ANO/NE)**	**Hodnota parametru účastníka** (odkaz na číslo stránky v produktovém listu/technické specifikaci apod.)
22	Pořízením je chápán nákup licencí SW (bez ohledu na to, zda se jedná o řešení „On-premise“ nebo SW využívá cloudového prostředí), implementace a následná technická a legislativní podpora. Součástí dodávky musí být všechny potřebné časově neomezené licence, včetně databázových, a musí splňovat bezpečnostní požadavky ZoKB (VoKB). Příslušné systémové licence budou registrovány na uživatele, jímž je Oblastní nemocnice Náchod a.s.	ano	ano
23	V případě, že SW nástroj využívá cloud, pak musí být součástí dodávky i licence poskytovatele cloudového úložiště. V tomto případě požaduje zadavatel od uchazeče před podepsáním smlouvy závazné prohlášení, že data uchazeče neopustí teritorium zemí EU a vztahuje se na ně ochrana podle zákona o ochraně osobních údajů GDPR.		V rámci dodávky nabízíme on-premis licenci k systému
24	Zadavatel požaduje časově neomezené licence pro minimálně 15 současně pracujících uživatelských licencí s možností jejich eventuálního rozšíření.	ano	V rámci dodávky poskytneme odpovídající počet licencí pro práci min. 15 souběžně pracujících uživatelů s možností jejich rozšíření dle potřeb zadavatele
Požadavky na implementaci SW:		**Splňuje (ANO/NE)**	**Hodnota parametru účastníka** (odkaz na číslo stránky v produktovém listu/technické specifikaci apod.)
25	Vstupní analýzu požadavků, konzultace, převod dat ze stávajícího systému ve formátu „xlsx“ v rozsahu 2 MD (pouze pro převod dat), konfiguraci a nastavení SW nástroje, testování, zaškolení a uvedení do rutinního provozu.	ano	Součástí dodávky bude analýza, migrace odpovidajích dat, customizace systému dle požadavků vyplývajích z analýzy, testování a zaškolení uživatelů, včetně uvedení do rutinního provozu. Jednotková cena za MD je uvedena v cenové příloze.
26	Součástí implementace musí být i integrace do Active Directory zadavatele a do e-learningového systému od společnosti Knowspread.cz s.r.o., provozovaný ve webovém prostředí v rozsahu práce 3 MD.	ano	Součástí dodávky bude integrace na AD a se systémem Knowspred dle požadavků zadavatele.
27	Součinnost s dodavatelem e-learningového systému (Knowspread) zajistí dodavatel formou subdodávky.	ano	Ano, uzavřeli jsme dohodu o spolupráci se společností provozující systém Knowspred umožňující výměnu odpovídajích dat pro potřeby integrace.
Požadavky na technickou a legislativní podporu v minálním rozsahu:		**Splňuje (ANO/NE)**	**Hodnota parametru účastníka** (odkaz na číslo stránky v produktovém listu/technické specifikaci apod.)
28	Nejnovější verzi systému od výrobce, legislativní shodu, a to nejenom s legislativou souvztažné ke kybernetické bezpečnosti a ochraně osobních údajů, telefonickou nebo emailovou technickou podporu v režimu 8/5, konzultace a školení nových verzí nebo programovací práce v rozsahu 3 MD/rok s možností převodu nevyčerpaných hodin nebo MD do dalšího období.	ano	V rámci služeb podpory(maitenance) je k dispozici uživatelský HelpDesk, pravidelný legislativní a bezpečností update systému. Po dohdě bude dostupná metodická a systémová podpora našich konzultantů dle vašich potřeb.
Systémové požadavky:		**Splňuje (ANO/NE)**	**Hodnota parametru účastníka** (odkaz na číslo stránky v produktovém listu/technické specifikaci apod.)
29	Účastník(dodoavatel) musí disponovat vlastním vývojovým prostředím, tedy případný vývoj i nových verzí probíhá u Účastníka, poté je implementován do testovacího prostředí Zadavatele (Objednavatele) a po odsouhlasení Zadavatelem je nasazen do produkčního prostředí. □	ano	Ano, ATTIS software s.r.o.je tvůrcem systému ATTIS a vlastníme veškerá autorská práva a disponujeme vlastním vývojovým a konzultačním týmem.
30	Systém obsahuje vlastní auditní logování s grafickým uživatelským rozhraním pro strukturované vyhledávání dle data a času, úkonů a uživatelů. Podpora předávání logů systému do logovacích systémů třetích stran.	ano	Systém ATTIS disponuje logováním vybraných aktivit. Disponuje také web API pro exporty auditních logů pro potřeby systémů třetích stran.
31	Zadavatel požaduje jako součást protokolu o převzetí zápis o provedení penetračního testu aplikace.	ano	Provedeme penetrační test.
32	V případě on-premise řešení provede dodavatel instalaci do infrastruktury ONN v součinnosti s techniky útvaru ICT zadavatele. Součinnost s technikem útvaru ICT musí být dodavatelem domluvena s minimálním předstihem 5 pracovních dnů, a to prokazatelným způsobem (email, zápis z jednání). Instalace bude provedena ve stávající virtuální infastruktuře VMware s licencováním MS Windows Server DataCenter 2019 a centrálním zálohovacím systémem Veeam. Dodaný server musí podporovat minimálně verzi VMware7. ONN netrvá na OS Microsoft, avšak musí splňovat bezpečnostní požadavky ZoKB (VoKB). Provoz fyzických serverů není z koncepčních a prostorových důvodů přípustný.	ano	ano

33	Vzdálený přístup za účelem instalace nebo následné podpory bude vždy realizován po domluvě a v součinnosti s technikem útvaru ICT pomocí stávajícího systému VPN na bázi aktuální aplikace FortiClient s dvoufaktorovou autentizací (token v SMS zprávě). Dodavatel v této souvislosti dodá útvaru ICT jmenný seznam vzdáleně přistupujících techniků včetně emailových adres a čísel mobilních telefonů. V případě personálních změn dodavatel musí tento seznam aktualizovat.	ano	ano
34	Systém i jeho dílčí části (moduly) komunikují v českém jazyce.	ano	ano
35	rozsahu zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, přičemž předaná dokumentace k systému musí odpovídat ustanovením vyhlášky č. 529/2006 Sb., část druhá, Provozní dokumentace, § 10 (je požadována pouze provozní dokumentace), § 11 (je požadována pouze provozní	ano	ano
36	**Předání elektronické verze bezpečnostní dokumentace v souladu s vyhláškou č. 82/2018 Sb. v minálně tomto rozsahu:**		
	Systémovou bezpečnostní politiku zpracovanou metodou GAP analýzy, tj. je požadována pouze dokumentace rozdílných vlastností oproti obecné bezpečnostní politice	ano	ano
	Definici hranic ISMS	ano	ano
	Plány obnovy IS	ano	ano
	Hodnocení aktiv a rizik	ano	ano

Pokud tato Technická specifikace nebo jiná část Zadávací dokumentace včetně všech jejích příloh obsahuje názvy určitých dodavatelů nebo výrobků, nebo patentů na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, zadavatel výslovně uvádí, že umožňuje použití i jiných, kvalitativně a technicky rovnocenných řešení, které budou splňovat požadavky na předmět plnění veřejné zakázky s ohledem na ZoKB a VoKB.

Účastník zadávacího řízení je povinen dle pokynů zadávací dokumentace kompletně vyplnit níže uvedené tabulky s požadavky na předmět plnění a učinit je součástí svojí nabídky. Účastník pravdivě uvede do jednotlivých prázdných kolonek (zvýrazněné buňky), zda jím nabízené zařízení splňuje či nesplňuje v plném rozsahu uvedený požadavek (ANO/NE). U parametrů, které jsou charakterizovány konkrétní kvantifikovatelnou hodnotou, je povinen tuto hodnotu uvést. Zadavatel je oprávněn si veškeré informace ověřit a vyžádat si předložení dokladů, které splnění parametrů jednoznačně dokládají. Uvedené požadavky jsou nepodkročitelné, tzn., že jejich nesplnění bude posouzeno jako nesplnění technických požadavků na předmět plnění daných zadávací dokumentací a povede k vyloučení účastníka ze zadávacího řízení.

Podáním nabídky se zavazujete k i plnění podmínek uvedených v ZoKB, VoKB a NIS 2 neboť Oblastní nemocnice Náchod je osobou povinnou podle §3, písm. g) zákona o kybernetické bezpečnosti.
Dodavatel se musí při zpracování osobních údajů řídit Zákonem č. 110/2019 Sb. a Nařízením EU 2016/679 (GDPR).
Uchazeč proto musí jednat řádně a v kontextu i výše uvedených právních předpisů v oblasti kybernetické bezpečnosti a ochraně osobních údajů.

Dodavatel je oprávněn nabídnout zboží s jinými parametry za podmínky, že se jedná o parametry objektivně lepší, resp. srovnatelně výhodnější než základní vymezení zadavatele. Méně výhodný parametr se považuje za nesplnění požadavku, ledaže se vejde do přípustné odchylky(+/- 10%) nebo se jedná o číselný přepis, který bude objasněn.

Link na uvedeou dokumentaci:
https://aurehd.azurewebsites.net/account/public/docs

V Oolomouci dne 27.06.2024

ATTIS
ATTIS software s.r.o.
Hanušova 100/10, 779 00 Olomouc
IČ: 25894978

.....
Ing. Alexandr Toloch, jednatel