Kooperativa
VIENNA INSURANCE GROUP

Rozšíření pojištění a připojištění

Připojištění a rozšíření pojištění se sjednávají se sublimitem plnění v rámci limitu pojistného plnění sjednaného pro základní pojištění, v případě pojištění odpovědnosti za újmu způsobenu vadou výrobku a vadou vykonané práce, která se projeví po jejím předání, event. v rámci sublimitu pro toto pojištění, je-li sjednán. Sublimit je horní hranicí plnění pojistitele z jedné pojistné události a současně v souhrnu ze všech pojistných událostí vzniklých z příčin nastalých během jednoho pojistného roku, není-li v pojistné smlouvě ujednáno jinak.

Připojištění odpovědnosti za újmu na věcech převzatých nebo na věcech nebo zvířatech užívaných

Připojištění odpovědnosti za újmu způsobenou na movité věci, kterou pojištěný převzal za účelem provedení objednané činnosti (např. opravy, úpravy, prodeje, úschovy, uskladnění nebo poskytnutí odborné pomoci) a odpovědnosti za újmu způsobenou na movité věci nebo zvířeti, které pojištěný oprávněně užívá. Připojištění se nevztahuje na újmu způsobenou na užívaném motorovém vozidle a převzatém zvířeti.

Připojištění se **nevztahuje** na odpovědnost za újmu způsobenou na převzatém motorovém vozidle, pokud jej pojištěný převzal, aby na něm provedl objednanou činnost (např. opravu), ne proto, aby provedl objednanou činnost s jeho pomocí (jako prostředku k provedení objednané činnosti).

Připojištění je sjednáno se sublimitem ve výši: **1 000 000 Kč.**

Připojištění nákladů zdravotní pojišťovny a orgánu nemocenského pojištění

Připojištění se vztahuje na:

- náhradu nákladů na hrazené služby vynaložené zdravotní pojišťovnou,
- regresní náhradu orgánu nemocenského pojištění v souvislosti se vznikem nároku na dávku nemocenského pojištění,

pokud taková povinnost vznikla v důsledku pracovního úrazu nebo nemoci z povolání, které utrpěl zaměstnanec pojištěného.

Připojištění je sjednáno se sublimitem ve výši: **5 000 000 Kč.**

Připojištění odpovědnosti za čistou finanční škodu

Připojištění odpovědnosti za škodu, která vznikla jinému jinak, než jako škoda na věci nebo na zvířeti, nebo jako škoda vyplývající z újmy na zdraví nebo na životě nebo ze škody na věci nebo na zvířeti.

Připojištění se vztahuje rovněž na čistou finanční škodu způsobenou vadou výrobku a vadou práce, která se projeví po jejím předání.

Připojištění je sjednáno se sublimitem ve výši: **500 000 Kč.**

Kooperativa
VIENNA INSURANCE GROUP

Připojištění náhrady nemajetkové újmy způsobené neoprávněným zásahem do práva na ochranu osobnosti

Připojištění povinnosti pojištěného poskytnout peněžitou náhradu nemajetkové újmy způsobené zásahem do práva na ochranu osobnosti, pokud byla přiznána pravomocným rozhodnutím soudu.
Připojištění je sjednáno se sublimitem ve výši: **500 000 Kč.**

Územní rozsah

Pojištění se sjednává s územním rozsahem: území **Evropy**.

* Toto potvrzení o pojištění je vystaveno na žádost pojistníka. Rozsah pojištění uvedený v tomto potvrzení je pouze informativní, přesný rozsah pojištění vyplývá z výše uvedené pojistné smlouvy, včetně pojistných podmínek a dalších smluvních dokumentů, které jsou její nedílnou součástí.

Ve Zlíně dne 4. 1. 2023

[redacted]
podpis zástupce pojistitele

[redacted]
podpis zástupce pojistitele

Žádost o povolení vzdáleného přístupu VPN k datové síti ÚVN

Jméno a příjmení		Firemní e-mail
Jméno externí firmy	**Firemní telefon**	**Mobilní telefon**

Odůvodnění žádosti ke vzdálenému přístupu VPN k datové síti ÚVN a specifikace období a požadovaných aplikací / serverů / služeb:
.....

.....

Žádám o poskytnutí vzdáleného přístupu do datové sítě ÚVN z důvodu plnění servisní smlouvy

ze dne: ..... Přístup na období od...../...../..... do...../...../.....
Při využívání tohoto přístupu budu zachovávat bezpečnostní doporučení a budu pracovat v souladu s touto smlouvou a nařízením Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů - GDPR a další související platné zákony.
Přístupové údaje budu udržovat v tajnosti a nikomu jinému neumožním využívání mého přístupu. V případě, že zjistím, že došlo k vyzrazení přístupových údajů, požádám ÚVN o jejich zablokování a vystavení nových přístupových údajů.

Žadatel svým podpisem stvrzuje, že výše uvedené podmínky bude plnit, a že je si vědom, že v případě porušení jakékoliv z výše stanovených povinností dojde k okamžitému odebrání přístupu a zahájení dalších adekvátních kroků ze strany ÚVN.

Dne ..... podpis žadatele .....

Stanovisko osoby odpovědné v ÚVN za plnění předmětné smlouvy: ☐ souhlasím ☐ nesouhlasím

Dne: ..... jméno a podpis .....

Stanovisko příslušného náměstka: ☐ souhlasím ☐ nesouhlasím

Dne: ..... jméno a podpis .....

Stanovisko vedoucího Odboru bezpečnosti a krizového řízení: ☐ souhlasím ☐ nesouhlasím

Dne: ..... jméno a podpis .....

Stanovisko vedoucího Odboru informatiky: ☐ souhlasím ☐ nesouhlasím

Dne: …… jméno a podpis ……..

Nastavení provedl a informace žadateli předal: ☐ nastavil ☐ nelze nastavit - důvod

Dne: …… jméno a podpis ……..

Technické a bezpečnostní požadavky na provoz v síti ÚVN

Technické a bezpečnostní požadavky pro provoz zařízení v síti ÚVN

Z důvodu určení ÚVN jako poskytovatele základní služby (součást kritické infrastruktury státu) musí každé řešení, informační systém a zařízení, včetně zařízení zdravotnické techniky zohledňovat bezpečnostní požadavky vyplývající ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti) jako je Vyhláška 82/2018 Sb. a Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, tzv. GDPR),
v české legislativě je přeneseno jako zákon č. 110/2019 Sb. (Zákon o zpracování osobních údajů).

Jde zejména o : **ANO/NE, příp. popis, jak bude zajištěno**

A. Obecné otázky zajištění kybernetické bezpečnosti

Požadavky	Splněno - ANO	Splněno - NE (náhradní řešení)
Možnost umístění do samostatné VLAN		NE – IP zůstane zachováno
Zabezpečení zařízení a sítě před kybernetickými útoky za účelem snížení rizika šíření škodlivého kódu a kybernetických útoků o **ochrana před škodlivým kódem (antivirus)** o **instalace bezpečnostních záplat** o **možnost inspekce SSL provozu**	ANO	
Administrátorský účet systému (admin, root, superuser) nesmí být využit jako provozní účet	ANO	
Každý uživatel musí mít samostatný účet ověřovaný oproti LDAP/MS Active directory ÚVN	ANO	

Používána je pouze zabezpečená komunikace		NE – DICOM protokol
B. Provozní kybernetická bezpečnost		
Požadavky	Splněno - ANO	Splněno - NE (náhradní řešení)
Systém musí ověřovat uživatele/skupiny vůči LDAP/Active Directory ÚVN	ANO	
Všechny provozované OS a SW musí umožňovat instalaci bezpečnostních patchů	ANO	*doporučené náhradní řešení je předřazený HW prostředek zajišťující kybernetickou bezpečnost, např. NGFW ve správě dodavatele*
Systém musí zaznamenávat (logovat) přístupy do systému a záznam zpřístupnit/odesílání logů do monitorovacího nástroje (SIEM)	ANO	
Systém umožní provozování antivirového řešení ÚVN za předpokladu, že Zadavatel zajistí jeho vhodnou konfiguraci.	ANO	
C. Provozní bezpečnost osobních a zdravotních údajů (informativní)		
Požadavky	ANO (příp. vypsat detaily/částečné splnění)	NE (příp. vypsat detaily/částečné nesplnění)
Může zařízení přenášet nebo uchovávat elektronické chráněné zdravotní informace (ePHI*)?		
Typy datových prvků ePHI, které může zařízení obsahovat (uchovávat, ukládat): a) demografické (jméno, adresa, lokalita, jedinečné identifikační číslo) b) zdravotní záznam (číslo záznamu, rodné číslo, číslo účtu, datum vyšetření, id zařízení) c) diagnostické/terapeutické (fotografie/radiografie, výsledky, fyziologická data) d) jiný otevřený nestrukturovaný text zadaný uživatelem/operátorem zařízení	a) ANO b) ANO c) ANO d) ANO	a) b) c) d)
Údržba ePHI: Zařízení může a) uchovávat ePHI dočasně v nestálé paměti (dokud není smazáno vypnutím/resetem) b) trvale ukládá ePHI na lokální médium (disk, paměť)	a) ANO b) ANO	a) b)

c) importuje/exportuje ePHI z jiných systémů/na jiné systémy	c) ANO	c)
Mechanismy používané pro přenos, import/export ePHI: Zařízení může a) zobrazovat ePHI (např. zobrazovat videa) b) generovat tištěné zprávy (reporty) nebo obrázky obsahující ePHI c) načítat ePHI z nebo zaznamenávat ePHI na vyměnitelná média (např. disk, DVD, CD-ROM, páska, CF/SD karta, paměťová karta) d) vysílat/přijímat či importovat/exportovat ePHI přes vyhrazené kabelové připojení (např. IEEE 1073, sériový port, USB, FireWire) e) vysílat/přijímat ePHI přes síťové připojení (např. LAN, WAN, VPN, intranet, internet) f) vysílat/přijímat ePHI přes integrované bezdrátové připojení (např. WiFi, Bluetooth, infračervené) * *ePHI: Electronic Protected Health Information; překlad: elektronické chráněné informace o pacientech, - pojem používaný pro pacientské záznamy vedené v elektronické podobě, čeština nemá zkratku.*	a) ANO b) ANO c) ANO d) ANO e) ANO f)	a) b) c) d) e) f) NE
D. Technická specifikace - Serverová část		
Serverová část je součástí dodávky		ANO - NE *
	Splněno - ANO	Splněno - NE (náhradní řešení)
Dodávaná serverová část systému musí být provozovaná na výrobcem OS podporované verzi.	ANO	
ÚVN disponuje licencemi MS Windows Server ve virtuálním prostředí Microsoft Hyper-V. ÚVN požaduje využití virtuálního prostředí Microsoft Hyper-V pouze Gen2. Bude v rámci dodávaného řešení tato licence využita?	-	
ÚVN provozuje virtuální servery RedHat compatibile minimálně verze 7. Bude v rámci dodávaného řešení toto využito?	ANO	
Obsahuje dodávaný OS Secure Boot?	ANO	

Operační systém pro virtuální server musí být instalován místně. Není podporováno dodání již hotového virtuálu.	-	
Oddělení informatiky ÚVN musí mít trvalý přístup do operačního systému: pro OS linux na úrovni root, pro operační systém Microsoft Windows na úrovni Local Administrators.	ANO	
Do operačního systému bude instalováno antivirové řešení ÚVN		NE
První disk v Microsoft operačním systému (typicky C:) je vyhrazen pouze pro potřeby operačního systému, pro ostatní potřeby bude připojen druhý a další disky.	-	
Operační systém i dodané služby musí běžet trvale a bez přerušení. Restarty operačního systému provádí pouze ÚVN.	ANO	
Systém musí ověřovat uživatele oproti Microsoft Active Directory nebo službě LDAPS	ANO	
V případě ověřování uživatelů protokolem LDAP musí být uživatel ověřován v LDAP stromu rekurzivně.	ANO	
V případě, že linuxový systém bude poskytovat sdílené adresáře, musí se v linuxovém systému ověřovat uživatelský účet oproti MS Active directory/ MS LDAPS	ANO	
V případě, že na serveru bude vyžadován běh služby, služba musí běžet pod doménovým účtem vytvořeným pro běh služby. Běh služby pod lokálním účtem je povolený pouze na platformě LINUX.	ANO	
Před započetím implementace budou dodány oddělení informatiky ÚVN následující informace: a) seznam instalovaných aplikací včetně jejich verzí b) všechna zakoupená sériová čísla produktů spojených s dodávkou c) jmenný seznam nainstalovaných služeb, s kým nebo čím služba komunikuje d) otevřené porty ve firewallu na serveru, s kým nebo čím port komunikuje e) odhadovaná velikost úložiště pro dodávané řešení po 1 roce a 10 letech obvyklého provozu dodávaného systému.	a) ANO b) ANO c) ANO d) ANO e) ANO	a) b) c) d) e)
webový prohlížeč: pouze Microsoft Edge Chromium v poslední vydané verzi	-	

ÚVN disponuje MS SQL 2022. Bude v rámci dodávaného řešení využita?	-	
Součástí dodávky jsou veškeré potřebné licence a technologie pro provoz včetně předání licenčních čísel a doložení legálnosti použitého SW písemnou formou.	ANO	
Dodávaný software na serverech i stanicích je funkční v doménovém prostředí Microsoft Active Directory s funkční úrovní domény minimálně Windows Server 2012.	ANO	
Dodávaný software na serverech i stanicích nesmí pro svůj běh požadovat zvýšené oprávnění (například local administrator práva, poweruser práva)	-	
E. Pracovní stanice připojená do sítě ÚVN (Pokud je součástí dodávky pracovní stanice pak bude uvedeno o jakou pracovní stanici se jedná)		
	Je součástí dodávky ANO - NE	Popis, název zařízení, které je předmětem dodávky
Součástí dodávky je Pracovní stanice víceúčelová připojená do sítě ÚVN (stanice na které mohou být provozovány i jiné sw než pouze pro potřeby dodávané ZT)	NE	
Součástí dodávky je Pracovní stanice výlučně sloužící pro účely ZT *(pozn. Pracovní stanice výlučně sloužící pro potřeby ZT a je určena pouze pro provoz aplikací související s provozem ZT a instalace jiného SW není výrobcem ZT povolena) – v tomto případě jsou tabulky „Požadavky na PC" a „Požadavky na monitory" irelevantní a nevyplňují se (očekává se dodávka jednoúčelové pracovní stanice sloužící pouze k napojení ZT a přenosu pacientských dat, která plní bezpečnostní a licenční požadavky na provoz zařízení v síti ÚVN).*	NE	
Technická specifikace - Pracovní stanice víceúčelová připojená do sítě ÚVN (bude vyplněno, pokud je v bodě E. vyplněno, že je součástí dodávky)		
HW, SW, licence	Splněno - ANO	Splněno - NE (náhradní řešení)
Pracovní stanice musí splňovat minimální HW požadavky pro provoz aplikace a současně minimální HW požadavky dle specifikace *(viz níže „Standardizované parametry ÚVN na PC a monitory v rámci centrálního nákupu")* včetně licence OS MS Windows.		
OS: minimálně Windows 11 Professional a vyšší s připojením do domény ÚVN		

Systém musí ověřovat uživatele oproti Microsoft Active Directory nebo službě LDAPS		
V případě ověřování uživatelů protokolem LDAP musí být uživatel ověřován v LDAP stromu rekurzivně.		
Do operačního systému bude instalováno antivirové řešení ÚVN		
Součástí dodávky jsou veškeré potřebné licence a technologie pro provoz včetně předání licenčních čísel a doložení legálnosti použitého SW písemnou formou.		
Dodávaný SW na pracovní stanice musí být provozovaný na výrobcem OS podporované verzi.		
Dodávaný software na stanicích je funkční v doménovém prostředí Microsoft Active Directory s funkční úrovní domény minimálně Windows Server 2012.		
V případě potřeby běhu služby pro dodávaný software na stanicích nesmí pro svůj běh požadovat zvýšené oprávnění (například local administrator práva, poweruser práva) a služba musí běžet popd doménovým účtem vytvořeným pro běh služby		
Činnost uživatele bude probíhat pod osobním uživatelským účtem řízeným MS Active Directory, který nevyžaduje zvýšené oprávnění.		
Budou-li na pracovní stanici ukládána pacientská data je dodavatel povinnen předat odladěný postup jejich zálohy a obnovy dat i SW řešení pro každý konkrétní případ během implementace.		
webový prohlížeč: pouze Microsoft Edge Chromium v poslední vydané verzi		
PC bude z hlediska OS (záplaty, antivirus) ve správě oddělení informatiky a je možné ji využít i pro instalaci a provoz jiných aplikaci (např. MS Office, NIS, atd.)		
Technická specifikace - Pracovní stanice výlučně sloužící pro účely ZT (bude vyplněno, pokud je v bodě E. vyplněno, že je součástí dodávky)		
Pracovní stanice výlučně sloužící pro potřeby ZT je určena pouze pro provoz aplikací související s provozem ZT a instalace jiného SW není výrobcem ZT povolena.	Splněno - ANO	Splněno - NE (náhradní řešení)
Pracovní stanice pro ZT nepotřebuje přístup do interní sítě ÚVN		
Pracovní stanice pro ZT nepotřebuje přístup na internet		
Podporované OS s možností instalace bezpečnostních záplat		
ověřování uživatele/skupiny vůči LDAP/Active Directory		
zajištění antivirového řešení, případně využití antivirových licencí ÚVN		

Dodávané řešení bude obsahovat zálohu pacientských dat minimálně po dobu 10 let		
F. Technická specifikace – vzdálený přístup	Je vyhovující možnost nabízeného vzdáleného přístupu ANO - NE	Popis požadovaného vzdáleného přístupu
Dodavateli bude umožněna vzdálená správa dodaného zařízení prostřednictvím vzdáleného přístupu s dvoufaktorovou autentizací konkrétních uživatelů ze strany dodavatele prostřednictvím VPN CheckPoint. Pokud je požadován jiný typ přístupu, je nutné jej popsat (VPN, tunel, S2S, https).		

* nehodící škrtněte

Standardizované parametry ÚVN na PC a monitory v rámci centrálního nákupu

Požadavky na PC:

Funkcionalita / požadované parametry závazné pro dodavatele		*min. / max.*	*Sestava PC* *Požadované parametry*	Nabízené PC *Navrhované parametry*
CPU (procesor)	Passmark CPU (www.passmark.com)	min.	Intel Core i3 12. generation nebo AMD Ryzen 5 5. generation	
		min.	4 fyzická jádra	
	Podpora rozšíření instrukční sady AES-NI		ano	
	Virtualizace procesoru a síťové karty		ano	
	Technologie 64 bit		ano	
Operační paměť	Typ	min.	DDR4	
	Celková instalovaná velikost	min.	16 GB	
	Možnost doplnění na celkovou velikost	min.	32 GB	

	podpora Windows 10 Virtualization-based Security (VBS) – VT-x, SLAT, VT-D, WSMT, UEFI MAT, EFI Page Protections, MOR v2 (nebo ekvivalentní)			ano	
Hlučnost zařízení	při požadovaných výkonech procesorů a při teplotě 23°C ± 2°C a měřena dle normy ISO 7779		max.	38 dB	
UEFI/BIOS	Identifikace UEFI (Unified Extensible Firmware Interface) / BIOS musí obsahovat sériové číslo a informace o výrobci a modelu			ano	
	Možnost zabezpečení heslem proti neoprávněnému přístupu do BIOS			ano	
	Podpora SecureBoot s kapacitou NVRAM minimálně 128 KB pro uložení klíčů (PK, KEK, db, dbx)			ano	
	Možnost zablokování zavedení operačního systému z periférií.			ano	
	Možnost zaměnit BIOS za UEFI (Unified Extensible Firmware Interface)			ano	
	Možnost zablokování vybraných zařízení (periférií) tak, aby s nimi nemohl pracovat OS.			ano	
	Identifikace UEFI (Unified Extensible Firmware Interface) musí obsahovat licenční kód k produktu OS			ano	
Pevný disk	SSD M2 slot	kapacita	min.	512GB	
		rychlost čtení / zápis MB / sec	min.	1200/1200	
Základní deska	Integrovaná síťová karta - 100/1000 Mbit/sec, RJ45, Wake on LAN, podpora "802.1X", PXE (Preboot eXecution Environment)			ano	
	Integrovaná grafická karta	rozlišení	min.	2560 x 1440	
		podpora práce více monitorů	min.	2	
		rozhraní	min.	2x digitální připojení k externímu monitoru (DP/HDMI standard) Displayport minimálně ve verzi 1.4 nebo HDMI minimálně ve verzi 2.0	
	Integrovaná zvuková karta			ano	
	min. TPM (Trusted Platform Module) chip verze TPM 2.0			ano	

	Integrovaná konektivita	USB (2.0 a vyšší)	min.	min. 7x - z toho vzadu min. 2x USB-A 3.1 (nebo vyšší), z toho vpředu min 2x USB-A 3.1 (nebo vyšší) a 1x USB-C	
		PCI / PCI Express (x16/x8)		ano	
		1x Jack konektor 3,5mm audio out a 1x Jack konektor 3,5mm audio in (může být společný)	min.	1	
Napájecí zdroj	Výkon odpovídající stabilnímu chodu sestavy			ano	
	Napájecí síťový kabel délky min. 1,5 m			ano	
Mechanika paměťových médií	Mechanika optických disků DVD DL ± RW interní nebo externí s možnosti připojení přes USB (včetně kabelů 1.5 m)			ano	
Skříň	Provedení			SFF	
	Zabezpečení: detekce vniknutí do skříně s hlášením			ano	
	Uzamykatelná			ano	
Externí kursorový ovladač (myš)	USB: min. 3 tlačítka, délka kabelu min. 1,5m, symetrické provedení (pro praváky i leváky), rolovací kolečko, senzor laser nebo BlueTrack min. 1000 DPI, klasická velikost od 10 do 12 cm (ne malé notebookové)			ano	
Externí klávesnice	USB: klasické rozložení CZ, klávesy F1-F12 a numerická klávesnice (tlačítko Enter a Shift zvětšené), české rozložení kláves, délka kabelu min. 1,5 m, klávesy s nízkým zdvihem, min. 101 kláves, protiskluzová úprava			ano	
Společné parametry					
Systémová platforma	Základní předinstalované programové vybavení (image na disku) - OS OEM MS Windows 11 Professional CZ 64 bit.			ano	
	Dodání CD/DVD/USB s operačním systémem, ovladači nebo managementem			ano	
Záruka	Záruka v ČR garantovaná výrobcem dokončení opravy NBD on-site od nahlášení, ponechání vadného disku zákazníkovi.		min.	5 let	

	Řešení závad - rozsah servisních středisek, telefonní podpora a podpora prostřednictvím internetu: Jediné kontaktní místo pro nahlášení poruch v celé ČR, servisní střediska pokrývající celé území ČR, možnost sledování servisních reportů prostřednictvím internetu. Podpora poskytovaná prostřednictvím telefonní linky (zdarma nebo běžný účastnický tarif) v českém /slovenském jazyce musí být dostupná v pracovní dny minimálně v době od 8:00 do 17:00 hod. Podpora prostřednictvím internetu musí umožňovat stahování ovladačů a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení nebo jiný unikátní identifikátor na zařízení.		ano	
Ostatní	Zařízení musí splňovat: Nařízení Komise EU č. 617/2013 ze dne 26. června 2013, kterým se provádí směrnice Evropského parlamentu a Rady 2009/2009/125/ES, soulad s direktivou RoHS (Restriction of Use of Certain Hazardous Substances), certifikát EPEAT (Electronic Product Environmental Assessment Tool), Energy Star min. 6.1.		ano	
	Sestava v odstínu jedné barvy (výběr z barev černá, šedá, bílá, stříbrná)		ano	

Požadavky na monitory:

Funkcionalita / požadované parametry závazné pro dodavatele	***min. / max.***	***Monitor k PC (minimální požadavky)***	***Nabízený Monitor***
		Požadované parametry	***Nabízené parametry***
Velikost úhlopříčky	min.	**23,8"**	
Technologie		LCD barevný, IPS	
Pracovní rozlišení bodů (š x v)	min.	1920 x 1080	
Povrh displeje		matný	
Podsvícení LED		ano	
Jas [cd/m2]	min.	250	

Kontrastní poměr (typický)		min.	1000:1	
Redukce (filtr) modrého světla			ano	
Pozorovací úhel (h x v)		min.	178°x178°	
Doba odezvy		max.	8 ms	
Rozhraní (konektory)	digitální port (HDMI a DisplayPort)	min.	2 (1x HDMI a 1x DP)	
Výškově nastavitelný stojan			ano	
Nastavení náklonu (předo-zadní)			ano	
Otočení monitoru o +/- 90 ° (pivot)			ano	
Napájecí síťový kabel délky min. 1,5 m a propojovací HDMI a DP kabel.			ano	
Integrované reproduktory, nebo sounbar s podporou připojení k monitoru			ano	
Záruka	Záruka v ČR garantovaná výrobcem dokončení opravy NBD on-site od nahlášení.	min.	3 roky	
Řešení závad a Servisní střediska	Řešení závad - rozsah servisních středisek, telefonní podpora a podpora prostřednictvím internetu: Jediné kontaktní místo pro nahlášení poruch v celé ČR, servisní střediska pokrývající celé území ČR, možnost sledování servisních reportů prostřednictvím internetu. Podpora poskytovaná prostřednictvím telefonní linky (zdarma nebo běžný účastnický tarif) v českém /slovenském jazyce musí být dostupná v pracovní dny minimálně v době od 8:00 do 17:00 hod. Podpora prostřednictvím internetu musí umožňovat stahování ovladačů a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení nebo jiný unikátní identifikátor na zařízení.		ano	

Ostatní	Zařízení musí splňovat: Nařízení Komise EU č. 617/2013 ze dne 26. června 2013, kterým se provádí směrnice Evropského parlamentu a Rady 2009/2009/125/ES, soulad s direktivou RoHS (Restriction of Use of Certain Hazardous Substances), certifikát EPEAT (Electronic Product Environmental Assessment Tool), Energy Star min. 6.1.		ano	
	Barva v odstínech a kombinacích barev černá, šedá, bílá, stříbrná.		ano	

Příloha č. 6 Kupní smlouvy

Základní bezpečnostní požadavky pro dodavatele ÚVN v oblasti IT a IS

1. **Bezpečnost informací (SŘBI)**

- Dodavatel se zavazuje začlenit systém řízení bezpečnosti informací (SŘBI) do svých procesů, seznámit se a dodržovat předpisy ÚVN, zahrnující ochranu důvěrnosti, dostupnosti a integrity zpracovávaných informací. Je vyžadováno, aby dodavatel prováděl pravidelná školení pro rozvoj bezpečnostního povědomí a definoval jasné postupy pro řešení bezpečnostních incidentů. Zároveň musí zajistit, aby všechny bezpečnostní standardy byly dodrženy i jeho subdodavateli.
- Dodavatel zajišťuje, že všechna bezpečnostní opatření jsou dodržována i v rámci spolupráce se subdodavateli.
- V rámci smluvního plnění je dodavatel povinen zajistit ochranu přenášených a uchovávaných informací v souladu s Dohodou o nezveřejnění informací (NDA) a Dohodou o úrovni služeb (SLA), což obnáší implementaci šifrování a pečlivé správy přístupových práv. Je rovněž povinen bezodkladně informovat ÚVN o jakýchkoli incidentech ohrožujících bezpečnost těchto informací.

2. **Oprávnění přístupu k datům**

- Dodavatel je povinen chránit neveřejné informace před neoprávněným přístupem, používat informace pouze pro účely plnění smlouvy a zajišťovat náležité zabezpečení osobních údajů a chráněných informací.
- Dodavatel je povinen zajistit mlčenlivost svých zaměstnanců, včetně zaměstnanců subdodavatelů o informacích souvisejících s předmětem smluvního plnění.
- Dodavatel je povinen přiřazovat přístupová oprávnění k datům ÚVN s ohledem na potřebu minimalizace rizik neoprávněného přístupu k aktivům ÚVN.
- Dodavatel je povinen zabezpečit, že udělená přístupová práva jsou určena vždy pro konkrétní pracovníky a nebudou sdílena mezi více osobami.
- Dodavatel je povinen zajistit, aby všechny osoby s přístupem k informacím a datům ÚVN chránily své autentizační údaje.
- V rámci každé žádosti dodavatele o udělení přístupu k datům a informacím ÚVN je dodavatel povinen specifikovat rozsah a účel požadovaného přístupu, včetně potřebné doby jeho platnosti.

3. **Autorství a licence**

- Dodavatel informuje ÚVN o autorství zdrojového kódu dodávaného informačního systému a jeho licenčních podmínkách v rámci smluvního plnění.
- Dodavatel se zavazuje řídit se pravidly ÚVN pro použití, úpravy a distribuci softwaru a stanovuje, jak bude s kódem a daty z informačního systému nakládáno po ukončení spolupráce.
- Dodavatel je povinen zajistit, že jakékoli využití softwaru třetích stran, včetně open source a komerčních řešení, bude v souladu s příslušnými licenčními dohodami a integrováno do předmětu plnění vůči ÚVN i bez porušení autorských práv.

4. **Kontrola a audit**

- Dodavatel je povinen, na vyžádání, umožnit ÚVN provádět audity k ověření plnění smluvních závazků, zejména v oblastech bezpečnostních opatření, správy subdodavatelů, nakládání s daty a řešení bezpečnostních incidentů.
- Audity mohou být realizovány přímo ÚVN, nebo prostřednictvím třetí strany, s předem dohodnutými termíny, stanovenou metodikou a podmínkami, včetně požadavků na přítomnost konkrétních osob.

- Dodavatel je povinen zajistit přístup auditorů k potřebným informacím a systémům a zavazuje se reagovat na výsledky auditů prostřednictvím přijetí a implementace nápravných opatření pro odstranění zjištěných nedostatků, vždy ve stanoveném termínu.

5. Řetězení dodavatelů

- Dodavatel je povinen zajistit, aby všichni subdodavatelé dodržovali bezpečnostní a smluvní ujednání stanovená v rámci smlouvy s ÚVN.
- Dodavatel je zodpovědný za veškeré činnosti subdodavatelů a musí garantovat, že jejich činnost je v souladu se smluvním předmětem plnění.
- ÚVN má právo, vůči dodavateli, schvalovat subdodavatele na základě předem stanovených kritérií, která jsou definována v rámci výběrového řízení.
- Dodavatel je povinen informovat ÚVN o změně subdodavatele, jehož činnost přímo souvisí s předmětem smluvního plnění vůči ÚVN.

6. Dodržování bezpečnostních politik

- Dodavatel je povinen dodržovat politiky ÚVN, zejména:
  - **a)** Systém řízení bezpečnosti informací (SŘBI),
  - **b)** Bezpečnostní politika informačních systémů (BPIS),
  - **c)** Politika řízení informačních aktiv (PŘIA),
  - **d)** Politika řízení lidských zdrojů v kybernetické bezpečnosti.
- Výše uvedené politiky jsou přikládány ke smlouvám s dodavateli formou příloh.
- Dodavatel je dále povinen se seznamovat s politikami ÚVN, které mají přímou souvislost s předmětem smluvního plnění (vzdálený přístup, zajištění fyzické bezpečnosti apod.)

7. Řízení změn

- Dodavatel je povinen řídit a informovat o změnách týkajících se předmětu plnění následujícím způsobem:
  - **a)** Všechny změny související s předmětem smluvního plnění musí být vzájemně schváleny ÚVN a dodavatelem.
  - **b)** Dodavatel se zavazuje postupovat podle předem stanovených procesů při zavádění změn, tento proces zahrnuje provedení a předložení analýzy možných dopadů změn, proces akceptace změn a testování před zavedením do běžného provozu.
  - **c)** Dodavatel garantuje, že je v případě potřeby ÚVN schopen zajistit možný návrat systému do původního stavu před aplikovanými změnami.

8. Soulad se zákony

- Dodavatel se zavazuje zajistit, že plnění předmětu smlouvy vůči ÚVN bude v souladu s aktuálními právními předpisy, zejména s těmi, které jsou přímo relevantní pro rozsah plnění smlouvy.
- Toto ujednání zahrnuje povinnost dodržovat všechny platné zákony, vyhlášky, nařízení, Evropské předpisy a obecně závazné vyhlášky, které souvisí s předmětem plnění.

9. Informování o incidentech

- Dodavatel je povinen ÚVN neprodleně informovat o jakýchkoliv bezpečnostních incidentech, které mají vztah k předmětu plnění smlouvy nebo mohou mít dopad na aktiva ÚVN.
- Dodavatel je povinen:
  - **a)** oznámit ÚVN výskyt bezpečnostního incidentu, souvisejícího s předmětem plnění smlouvy, ihned po jeho detekci.
  - **b)** poskytnout ÚVN informace o bezpečnostním incidentu v takové formě, aby byla ÚVN schopna rychle a efektivně reagovat na vzniklou bezpečnostní hrozbu.
  - **c)** dodržet lhůtu pro informování ÚVN o vzniku bezpečnostního incidentu, která nesmí přesáhnout 24 hodin od jeho detekce.

10. Informování o řízení rizik

- Dodavatel je povinen informovat ÚVN o metodách a procesech řízení rizik, které uplatňuje ve vztahu k předmětu smluvního plnění. Toto informování zahrnuje:
    - **a)** popis identifikace, hodnocení a minimalizace rizik včetně příkladů konkrétních opatření;
    - **b)** informování ÚVN o zbytkových rizicích, která zůstávají i po zavedení nápravných opatření, s uvedením možných negativních dopadů na ÚVN v rámci smluvního plnění;
    - **c)** informování ÚVN o změnách v procesu řízení rizik nebo při objevení nových;
- Dodavatel umožní ÚVN provádět kontroly a audity procesů řízení rizik v souladu s postupy specifikovanými v bodě č. 4 tohoto dokumentu.

11. Informování o významných změnách

- Dodavatel se zavazuje bezodkladně informovat ÚVN o všech významných změnách, které mohou výrazně ovlivnit jeho schopnost splnit smluvní závazky nebo bezpečnost poskytovaných služeb, včetně:
    - **a)** změn ve vlastnické struktuře nebo řízení společnosti;
    - **b)** převodu aktiv důležitých pro předmět smluvního plnění;
    - **c)** změn, jež se týkají práv a povinností v souvislosti s těmito aktivy.

12. Právo odstoupit od smlouvy

- ÚVN si vyhrazuje právo odstoupit od smlouvy bez sankcí v případě, kdy nastanou zásadní změny ve struktuře ovládaní dodavatele nebo ve vlastnictví klíčových aktiv, které jsou pro plnění smlouvy kritické. Významná změna se vztahuje na ovládání nebo řízení dodavatele v souladu s platnou legislativou[1].

13. Bezpečnost při ukončení smlouvy

- Dodavatel je povinen při ukončení smlouvy přijmout následující kroky za účelem zajištění bezpečnosti a kontinuity služeb pro ÚVN:
    - **a) Zajištění přechodného období:**
      Dodavatel pokračuje v poskytování nezbytných služeb po dobu potřebnou k zajištění hladkého přechodu na nového dodavatele nebo dokud nebude ÚVN schopno fungovat bez jeho pomoci.
    - **b) Předání dat:**
      Veškerá data, včetně dokumentace provozních informací, je dodavatel povinen předat ÚVN nebo novému dodavateli v souladu s bezpečnostními standardy.
    - **c) Součinnost s novým dodavatelem:**
      V případě ukončení smlouvy s ÚVN je dodavatel povinen poskytnout součinnost novému dodavateli k zajištění plynulého převodu služeb a technologií.

14. Řízení kontinuity činností

- Dodavatel se zavazuje ke spolupráci v rámci řízení kontinuity činností, tato součinnost zahrnuje:
    - **a)** Dodavatel poskytuje součinnost v rámci plánování kontinuity činností ÚVN, dodavatel jasně definuje poskytované služby a je připraven na možné krizové situace (mimořádné události apod.).
    - **b)** Role, úkoly a odpovědnosti dodavatele jsou specifikovány v havarijních plánech ÚVN a v plánech pro obnovu provozu.
    - **c)** Smluvní plnění definuje, jaké operace a služby dodavatele mohou být ovlivněny v případě vzniku mimořádné události, popřípadě krizových stavech.