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 D. 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*	Nabízené PC
			Požadované parametry	*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	

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.

15. Formát předání dat

- Dodavatel garantuje, že veškerá data a informace jsou předávána ÚVN v čitelných formátech a umožňují snadnou integraci do systémů ÚVN.

16. Likvidace dat

- Dodavatel se zavazuje k bezpečné likvidaci všech dat a provozních údajů ÚVN při ukončení smluvního plnění, a to v souladu s pravidly stanovenými v Politice řízení informačních aktiv (PŘIA), odkazované v bodě č. 6 tohoto dokumentu, a dle požadavků platné legislativy[7].

17. Sankce

- Dodavatel je povinen dodržovat veškeré smluvní povinnosti v oblasti kybernetické bezpečnosti. V případě porušení těchto povinností smlouva definuje sankce, které jsou úměrné hodnotě aktiv, poskytovaných služeb a možnému dopadu na ÚVN.
- Sankce mohou zahrnovat finanční pokuty, náhradu škody, odstoupení od smlouvy.