SMLOUVA O VÝPŮJČCE

uzavřená dle § 2193 a násl. zák. č. 89/2012 Sb., občanského zákoníku, v platném znění

Půjčitel: IMEDEX s.r.o.
se sídlem: Kladská 1092/1a, Hradec Králové, 500 03
zast.: [redacted]
IČ: 27510204 DIČ: CZ27510204
reg. v OR: u Krajského soudu v Hradci Králové, oddíl C vložka 23219
ID schránky: h2xbnd9
reg. č. distributora (prodejce): 014699_dis
reg. č. osoby provádějící servis: 014699_ser
reg. č. zdravotnického prostředku v informačním systému zdravotnických prostředků (dle zákona o zdravotnických prostředcích a diagnostických prostředcích in vitro č. 375/2022 Sb.): 00648317

Vypůjčitel: **Fakultní nemocnice Hradec Králové**
se sídlem: Sokolská 581, 500 05 Hradec Králové – Nový Hradec Králové
zast.: MUDr. Alešem Hermanem, Ph.D., ředitelem
IČ: 00179906 DIČ: CZ00179906
ID schránky: v7zqi84

Čl. I - Předmět výpůjčky

1. Tato smlouva se uzavírá na základě výsledků výběrového řízení s názvem **„Dodávka spotřebního materiálu na vyšetření refluxní epizody včetně. zápůjčky přístroje“**. Předmětem této smlouvy je závazek půjčitele přenechat vypůjčiteli k bezplatnému užívání zdravotnický prostředek: Restech Dx-1000 pH Measurement system, v. č. 3416, cena: 344 850,00,- Kč vč. DPH (dále jen „předmět výpůjčky).

2. Nedílnou součástí výpůjčky je:

   - instalační protokol,
   - doklad o instruktáži (proškolení) obsluhy,
   - doklad osoby, která je poučena výrobcem nebo osobou výrobcem pověřenou k provádění instruktáže daného zdravotnického prostředku (§ 41 zákona č. 375/2022 Sb., o zdravotnických prostředcích a diagnostických zdravotnických prostředcích in vitro),
   - doklady osob, které jsou proškoleny výrobcem nebo osobou výrobcem pověřenou k provádění servisu zdravotnického prostředku (§ 44, 45, 46 zákona č. 375/2022 Sb., o zdravotnických prostředcích a diagnostických zdravotnických prostředcích in vitro),
   - návod k obsluze zdravotnického prostředku v českém jazyce 2x (1x pro potřeby pracoviště v listinné podobě, 1x pro potřeby Oddělení nákupu zdravotnické techniky v elektronické podobě)
   - ES prohlášení o shodě výrobku (EC Declaration of Conformity) dle zákona č. 22/1997 Sb. v platném znění; pro zdravotnické prostředky tříd I sterilní, I měřící, IIa, IIb nebo III musí být CE doplněno číslem Notifikované osoby,
   - na zdravotnický prostředek, případně na všechny jeho komponenty, musí být v prohlášení o shodě (eventuálně v jiném písemném dokladu, který bude též součástí výpůjčky a bude potvrzen půjčitelem) uvedena třída zdravotnického prostředku,
   - pokud se výpůjčka skládá z více samostatných komponent, jsou její součástí platná prohlášení o shodě na všechny komponenty výpůjčky,
   - na všechny doklady předkládané v jiném, než v českém jazyce je součástí výpůjčky též jejich český překlad, za jehož správnost odpovídá půjčitel,

- platný protokol o provedené bezpečnostně technické kontrole v souladu se zákonem č. 375/2022., o zdravotnických prostředcích a diagnostických zdravotnických prostředcích in vitro,
- platná revize v souladu se zákonem č. 375/2022 Sb., o zdravotnických prostředcích a diagnostických zdravotnických prostředcích in vitro, případně další kontroly (revize) v souladu s tímto zákonem,
- předmět výpůjčky musí plnit požadavky přílohy č. 2: Požadavky na zapojení a provoz počítačů/zařízení v datové síti FN HK.

3. Zpracování osobních údajů dle Nařízení EU 2016/679 – obecné nařízení o ochraně osobních údajů (dále jen „GDPR“) viz Čl. V:

Varianta č. 1 – ANO ☒ NE ☐ **Varianta č.** 2 – ANO ☐ NE ☒

Čl. II - Doba výpůjčky

1. Vypůjčitel je oprávněn užívat předmět výpůjčky ode dne předání, instalace a provedení instruktáže obsluhy po dobu **neurčitou**.

Čl. III - Místo a podmínky převzetí předmětu výpůjčky

1. Půjčitel oznámí vypůjčiteli termín předání předmětu výpůjčky, a to Oddělení nákupu zdravotnické techniky tel. 495 833 265 a zároveň zástupci přebírajícího pracoviště dle Čl. III odstavec 2 minimálně 3 pracovní dny předem.

2. Místem předání předmětu výpůjčky je **ORL v sídle zadavatele**.

3. Oddělení nákupu zdravotnické techniky je až do dokončení instalace a předání zdravotnického prostředku do provozu jediným pracovištěm vypůjčitele oprávněným ke všem jednáním o dodávce a instalaci předmětu výpůjčky.

4. **V případě konektivity do datové sítě vypůjčitele je nutné bezodkladně po podpisu smlouvy, nejdéle však 4 týdny před plánovanou instalací, informovat IT oddělení vypůjčitele na adrese helpdesk@fnhk.cz. Oznámení o skutečném datu instalace je nutné provést nejdéle 3 pracovní dny předem.**

Čl. IV - Práva a povinnosti smluvních stran

1. Půjčitel prohlašuje, že předmět výpůjčky nemá žádné patentní nebo jiné právní vady, odpovídá všem platným právním předpisům a normám, je podle právních předpisů způsobilý k použití při poskytování zdravotních služeb a byla u něj podle právních předpisů posouzena shoda jeho vlastností se základními požadavky na zdravotnické prostředky s přihlédnutím k určenému účelu použití a výrobce nebo jeho zplnomocněný zástupce vydali písemné prohlášení o shodě.

2. Půjčitel je povinen zajistit vypůjčiteli servis a pravidelné kontroly event. validace předmětu výpůjčky v souladu se zákonem č. 375/2022 Sb., o zdravotnických prostředcích a diagnostických zdravotnických prostředcích in vitro, v platném znění, na vlastní náklady po dobu výpůjčky, a to od doby uvedení do provozu s tím, že opravy předmětu výpůjčky budou prováděny dle možností půjčitele v co nejkratší době.

3. Půjčitel má právo na provedení kontrol u vypůjčitele, a to za účelem provádění oprav na předmětu výpůjčky, vč. preventivních prohlídek, a za účelem kontroly užívání předmětu výpůjčky vypůjčitelem.

4. Vypůjčitel je povinen předmět výpůjčky řádně užívat, chránit jej před poškozením, ztrátou nebo zničením.

5. Vypůjčitel je povinen předmět výpůjčky vrátit půjčiteli ve stavu, v jakém jej převzal, s přihlédnutím k obvyklému opotřebení.

Čl. V - Ochrana osobních údajů

1. **Varianta 1 – osobní údaje se neukládají ani nepřenášejí ani k nim není umožněn přístup:** Půjčitel prohlašuje, že předmět výpůjčky neobsahuje žádná datová úložiště, do kterých by byly ukládány osobní údaje, ať už pacientů, obsluhujícího personálu nebo jiných fyzických osob, ani není vybaven na připojení k takovýmto úložištím.

2. **Varianta 2 – osobní údaje se ukládají nebo přenášejí nebo je k nim umožněn přístup:** Předmět výpůjčky obsahuje software a datová úložiště, umožňující ukládat a/nebo přenášet osobní údaje pacientů, obsluhy nebo osobní údaje jiných fyzických osob (subjekty údajů) nebo je k údajům umožněn osobní nebo elektronický přístup za účelem servisních nebo jiných služeb dle smlouvy.

3. Osobní údaje budou ukládány/přenášeny… … … … (místo, způsob, zálohování…doplní půjčitel).

4. Rozsah zpracování osobních údajů:
   a) **Povaha a účel zpracování**: *především ukládání, uspořádání, vyhledávání, přizpůsobení nebo pozměnění, nahlédnutí, zpřístupnění přenosem, osobní přístup, výmaz.*
   b) **Typ osobních údajů**: *kontaktní údaje, údaje o zdravotním stavu pacientů.*
   c) **Kategorie osobních údajů**: *osobní údaje, zvláštní kategorie osobních údajů.*
   d) **Doba trvání zpracování údajů**: dle doby platnosti smlouvy o výpůjčce zdravotnického prostředku.

5. V případě konektivity do datové sítě vypůjčitele bude předmět výpůjčky včetně jeho připojení do sítí elektronických komunikací a informačních systémů disponovat pouze takovými vlastnostmi, které podporují zajištění kybernetické bezpečnosti vypůjčitele v souladu s předpisy o kybernetické bezpečnosti.

6. Přístup k uloženým/přenášeným osobním údajům ze strany půjčitele bude omezen na minimální nezbytný rozsah a oprávněné osoby, které určí půjčitel. Půjčitel nebude bez vědomí vypůjčitele provádět kopie osobních údajů.

7. Pokud půjčitel poruší své povinnosti při ochraně osobních údajů, odpovídá za toto porušení vypůjčiteli, včetně nároků na náhradu případné škody.

8. Povinnost mlčenlivosti a ochrany osobních údajů trvá bez ohledu na ukončení platnosti této smlouvy.

9. Půjčitel bude při instalaci výpůjčky, zaškolení/instruktáže obsluhy a/nebo provádění záručního/pozáručního servisu provádět zpracování výše uvedených osobních údajů. Půjčitel jako zpracovatel toto zpracování omezí na nezbytný odpovídající rozsah a bude při něm dodržovat GDPR a zákon o zpracování osobních údajů č. 110/2019 Sb., v platném znění.

10. Zpracování zpracovatelem se řídí tímto ujednáním, které písemně zavazuje zpracovatele dle čl. 28 GDPR vůči správci (vypůjčitel). Tato ujednání stanoví, že zpracovatel:

a) zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně předání osobních údajů do třetí země nebo mezinárodní organizaci;
b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, pokud se na ně mlčenlivost již nevztahuje ze zákona;

c) s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, přijme se správcem vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
   - pseudonymizace a šifrování osobních údajů;
   - schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
   - schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
   - procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění zabezpečení zpracování;
   - opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce,

   přičemž se při posuzování vhodné úrovně zabezpečení zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim;
d) zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce;
e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů;
f) zpracovatel je správci nápomocen při zajišťování souladu s povinnostmi podle GDPR, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici, zejména pak je zpracovatel povinen, jakmile zjistí porušení zabezpečení osobních údajů, ohlásit jej bez zbytečného odkladu správci (e-mail DPO FN HK: **gdpr@fnhk.cz**);
g) zpracovatel po splnění účelu smlouvy všechny osobní údaje vymaže nebo je, je-li to možné, vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie;
h) poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené pro zpracovatele dle GDPR, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a těchto auditů se bude aktivně účastnit;
i) zpracovatel informuje neprodleně správce v případě, že podle jeho názoru určitý pokyn porušuje toto nařízení nebo jiné předpisy na ochranu osobních údajů;
j) pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy stejné povinnosti na ochranu osobních údajů, jaké jsou uvedeny ve smlouvě mezi správcem a prvotním zpracovatelem, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky GDPR (neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany osobních údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel).

11. Technická a organizační opatření k ochraně osobních údajů:
    Zpracovatel přijal a zavazuje se udržovat po celou dobu zpracování dle této smlouvy vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající daným rizikům pro práva a svobody subjektů údajů, a to zejména v oblastech:
    a) Kontrola vstupu
    Zabezpečení systémů pro zpracovávání osobních údajů před přístupem neoprávněných osob, např. prostřednictvím identifikačních čipových karet, klíčů, elektrických otvíračů dveří, bezpečnostní služby a/nebo vrátného, alarmu, videosystémů apod.;
    b) Kontrola přístupu
    Zabezpečení systémů před neoprávněným použitím, např. prostřednictvím (bezpečnostních) hesel, mechanismů automatického zamykání, dvoufaktorového ověřování přístupu do informačních systémů, šifrování nosičů údajů apod.;
    c) Kontrola přístupových oprávnění

Zabezpečení, aby osoby bez příslušného oprávnění nemohly údaje číst, kopírovat, upravovat či vymazávat, např. prostřednictvím autorizačních konceptů, přístupových práv na základě příslušných potřeb a evidence přístupů;
d) Pseudonymizace
Zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření (např. databáze označená kódem, přičemž kód má vždy pouze Vypůjčitel).
e) Kontrola zpřístupňování osobních údajů
Zabezpečení, aby v průběhu elektronického přenosu nebo přepravy nemohly osoby bez příslušného oprávnění tyto údaje číst, kopírovat, upravovat či vymazávat, např. prostřednictvím šifrování, virtuálních privátních sítí (VPN), elektronického podpisu apod.;
f) Kontrola zadávání osobních údajů
Zajištění, aby bylo možné zpětně ověřit a zjistit, zda a kým byly osobní údaje do systémů pro zpracovávání údajů zadány, upravovány nebo z těchto systémů vymazány, např. prostřednictvím evidence oprávnění, vedení záznamů o zadávání osobních údajů apod.
g) Kontrola dostupnosti
Ochrana osobních údajů před náhodným nebo úmyslným zničením a/nebo ztrátou, např. prostřednictvím zálohování (online/offline; on-site/off-site), nepřerušitelných zdrojů napájení (UPS), antivirové ochrany, firewallů, zaznamenávání přenosových tras a krizových plánů;
h) Schopnost obnovit dostupnost osobních údajů (např. ze zálohy).
i) Řízení ochrany osobních údajů.
j) Řízení reakcí na incidenty.
k) Výchozí nastavení, která zajišťují standardní ochranu údajů.
l) Kontrola smluvních stran (řízení dodavatelů).

Čl. VI - Závěrečná ujednání

1. Právní vztahy založené touto smlouvou a v této smlouvě výslovně neupravené se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., v platném znění (zejména jeho § 2193 a násl.).

2. Předčasné ukončení platnosti této smlouvy je možné na základě písemné dohody smluvních stran. Předčasné ukončení platnosti této smlouvy je rovněž možné na základě výpovědi jednou ze smluvních stran s dvouměsíční výpovědní dobou. Výpověď musí být písemná, není třeba ji odůvodňovat, výpovědní doba začíná běžet od prvého dne měsíce následujícího po doručení výpovědi druhé smluvní straně.

3. Smluvní strany shodně prohlašují, že tato smlouva nebyla uzavřena adhezním způsobem a že se nejedná o smlouvu formulářovou, tzn., že na právní poměr uzavřený touto smlouvou nebude aplikován § 1798 občanského zákoníku.

4. Smluvní strany se dohodly, že v rámci smluvního vztahu založeného touto smlouvu bude aplikován § 2197 občanského zákoníku, tzn., že vypůjčitel je oprávněn kdykoli vrátit předmět výpůjčky půjčiteli.

5. Smluvní strany souhlasí s uveřejněním smlouvy dle zákona č. 340/2015 Sb., o registru smluv.

6. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran.

7. Tato smlouva může být doplňována či měněna pouze na základě písemných dodatků, akceptovaných oběma smluvními stranami.

8. Tato smlouva je vyhotovena v listinné podobě ve dvou stejnopisech, z nichž 1 stejnopis obdrží půjčitel a 1 stejnopis vypůjčitel. Smlouva též může být vyhotovena v elektronické podobě

v jednom vyhotovení a podepsána v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

9. Smluvní strany prohlašují, že tato smlouva vyjadřuje jejich svobodnou, pravou, vážnou a úplnou vůli, prostou omylů. Na důkaz shora uvedeného připojují oprávnění zástupci smluvních stran své podpisy.

Příloha č. 1: Popis výpůjčky
Příloha č. 2: Požadavky na zapojení a provoz počítačů/zařízení v datové síti FN HK

Za vypůjčitele:
v Hradci Králové dne: 06.01.2026

[redacted]

Fakultní nemocnice Hradec Králové

Za půjčitele:
v Hradci Králové dne: 05.01.2026

[redacted]

IMEDEX s.r.o.

[redacted]

IMEDEX s.r.o.
Kladská 1092/1a
500 03 Hradec Králové

pHmetrický systém pro detekci laryngo-faryngeálního refluxu RESTECH™

Ambulatorní systém Restech detekuje významné refluxní epizody aerosolového i kapalného obsahu do laryngo-faryngeální oblasti. Zde díky působení kyselých složek refluxátu dochází k poškození přilehlých tkání a orgánů.

Systém Restech se skládá z ambulatorního záznamníku, sondy a softwarového vybavení.

Záznamník Restech je kompaktní, snadno ovládané zařízení, pomocí kterého pacient udává změny polohy těla, vymezuje období jídla a zaznamenává subjektivní obtíže ve sledovaném časovém úseku zpravidla po dobu 24 hodin.

Sonda Restech je zavedena do oblasti za uvulu, kde je pomocí senzoru velice citlivého na pH zaznamenávána jeho změna. Inovací metody je schopnost zachytit i mikročástice evaporujícího refluxátu, které kondenzují na stěnách sliznic zejména Larynx a Pharynx.

Sonda je bezdrátově připojena k záznamníku, čímž není prakticky omezen aktivní způsob života sledovaného pacienta po dobu měření.

Softwarové vybavení systému Restech automaticky vyhodnocuje hodnoty měřeného pH a sleduje výskyt hodnoty pod stanoveným prahem pH 5,5 resp. 5,0, které bylo stanoveno jako prahová hodnota. Tato hodnoty jsou výchozím zdrojem pro kalkulaci Ryan skóre, které podobně jako DeMeester skóre /GERD/ vypovídá o patologii sledovaného pacienta.

+420 495 260 286
www.imedex.cz
imedex@imedex.cz

IMEDEX s.r.o.
Kladská 1092/1a
500 03 Hradec Králové

Systém Restech Dx-1000®:

- 24 až 48 hodinový monitoring pH v oblasti hltanu	ANO	rekordér Dx-Recorder™ (Dx-500), napájení 2xAA alkalické baterie
- zařízení pro bezdrátový přenos signálu do rekordéru	ANO	Dx-Transmitter™ (Dx-300) spojení sondy pomocí miniUSB konektoru, napájení 1x3V knoflíková baterie
- nastavitelná doba měření	ANO	volitelná doba měření 24 až 48 hod.
- záznam studie na SD kartu	ANO	data jsou zaznamenávána rekordérem Dx-500 na SD® Memory Card (Dx-064) pro přenos dat lze použít SD Memory Card Reader (Dx-065; součást systému)
- možnost záznamu času jídla, polohy a symptomů	ANO	7 uživatelských tlačítek – poloha, jídlo, symptom pálení, symptom kašel a 3 další volitelná symptomová tlačítka
- automatické vyhodnocení záznamu	ANO	Restech DataView™ (součást systému), automatická analýza dat, snadná editace, tisk reportu
- sonda pro měření pH v oblasti hltanu	ANO	možnost využití dvou typů antimonových sond Dx-pH Probe™ (Dx-201) a Dx-pH Lond Probe™ (Dx-201L)
- propojení se spánkovou laboratoří	ANO	pro propojení se spánkovou laboratoří slouží Dx-Sleep Adapter™ (Dx-400)

+420 495 260 286
www.imedex.cz
imedex@imedex.cz

IMEDEX s.r.o.
Kladská 1092/1a
500 03 Hradec Králové

Ostatní:

Instalace a zaškolení obsluhujícího personálu v rozsahu min. 4 hod.	ANO	
záruční doba na hardware 24 měsíců	ANO	

Minimální požadavky na pracovní stanici:

Operační systém	Windows 7 nebo vyšší
Procesor	Intel Pentium® Dual-Core nebo ekvivalentní
Operační paměť	512 MB
Volné místo na disku	410 MB pro program; 6 MB pro každou studii
Čtečka paměťových karet	Kompatibilní s SD paměťovou kartou

Příloha č. 2: Požadavky na zapojení a provoz počítačů/zařízení v datové síti FN HK

Dne 28. 7. 2025 ver. 9_9

Týká se počítačů/zařízení připojených do interní sítě FN HK

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno, podle § 22a odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, v řízení ve věci určení Fakultní nemocnice Hradec Králové, sídlem Sokolská 581, 500 05 Hradec Králové, IČO: 00179906, jakožto účastníka řízení podle § 27 odst. 1 písm. b) zákona č. 500/2004 Sb., správního řádu, ve znění pozdějších předpisů, provozovatelem základní služby a určení informačního systému, na kterém je tato základní služba závislá, informačním systémem základní služby, **dne 18. října 2018 rozhodl**, že Fakultní nemocnice Hradec Králové, sídlem Sokolská 581, 500 05 Hradec Králové, IČO: 00179906, **je správcem a provozovatelem základní služby**: Poskytování zdravotních služeb. Informační systém, na kterém je tato služba závislá, je informačním systémem základní služby.

Instalační standardy kyberbezpečnosti FN HK:

a) Počítače musí být s operačním systémem min. Windows 11 Prof CZ a vyšší (Windows 11 Home jsou nepřípustné) a jsou součástí domény MS Active Directory fnhk.cz
b) Na koncových stanicích Windows musí mít uživatel práva pouze jako user. Uživatelé musí být autorizováni proti MS Active Directory fnhk.cz.
c) Uživatel musí být autorizován loginem a heslem (nepřipouští se jeden anonymní účet pro všechny uživatele). Každý zaměstnanec FNHK má přidělen jeden unikátní login.
d) Na počítači/zařízení musí být instalován antivirový program FN HK s centrální správou. Aktuální antivirový program používaný ve FN HK.
e) Systémové služby aplikace **musí být spouštěny na pozadí** bez nutnosti spouštět je pod přihlášeným uživatelem.
f) Share adresáře jsou centrální a jsou tedy upřednostňovány. Výjimky je nutno žádat na oddělení výpočetních systému FNHK.
g) Jakékoliv vystavené služby nebo zdroje v datové síti FNHK musí být autorizovány loginem a heslem proti MS Active Directory fnhk.cz.
h) Koncové stanice uživatelů nesmí zastávat funkci serverů. Zejména aplikační a databázové servery musí být provozovány na vyhrazených serverech dle standardů FN HK.
i) Veškeré webové služby musí být realizovány jako TLS v minimální verzi 1.2. Certifikáty poskytuje OVS FN HK.
j) Veškeré bezdrátové komunikace WiFi musí být provozovány na WPA3.
k) Pro autorizaci WiFi preferujeme MS AD. Na odchylky musí být v nabídce zřetelně upozorněno.
l) Záložní zdroje (UPS) dodávané do FN HK pro systémy, které mají dopad na provoz pracoviště a jsou provozovány nepřetržitě, je vyžadováno napojení na datovou síť se zajištěním monitoringu přes Simple Network Management Protocol (dále jen „SNMP“) modul dle RFC 1628
m) Čas se synchronizuje z domény nebo z lokálních NTP serverů FN HK
n) Počítač/zařízení musí mít instalovaného klienta desktop managementu, kterým je plošně zajišťována aktualizace operačního systému a instalovaných aplikací. Aktualizační balíčky aplikací si zajišťuje dodavatel aplikace na vlastní náklady.
o) Administrátorské heslo musí odpovídat bezpečnostním standardům FN HK, délka minimálně 17 míst, velká a malá písmena, čísla, spec. znaky, změna hesla minimálně 1x za 18 měsíců
p) Systém musí být napojen na SIEM FN HK
q) Pro identifikaci v datové síti bude lokální firewall umožňovat minimálně ICMP ECHO (ping)
r) Veškeré SW příslušenství, které tvoří nedílnou součást předmětu plnění (např. operační systém, který tvoří nedílnou součást dodávaného zařízení, ovládací SW atd.), musí být v poslední (nejnovější) verzi, kterou výrobce SW k datu podání nabídky nabízí na trhu a výrobce zařízení v rámci svého produktového portfolia taková zařízení nabízí (tzn. dodavatel je povinen vždy dodat

takové zařízení, ve kterém výrobce zařízení používá k datu podání nabídky nejnovější verzi SW příslušenství). K dodanému SW příslušenství musí být dostupná bezplatná plnohodnotná technická podpora. Součástí technické podpory musí být průběžné provádění aktualizací SW (update, upgrade), včetně zajišťování aktualizace zabezpečení, opravy hotfix atd. Technická podpora musí být zajištěna bezplatně po dobu platnosti uzavřené servisní smlouvy. V případě, že v průběhu platnosti servisní smlouvy bude ze strany výrobce SW ukončena celosvětově technická podpora a dodavatel nebude schopen z technických důvodů zajistit u dodaného zařízení bezplatný upgrade na novější verzi systému s platnou technickou podporou, bude dodavatel povinen v rámci servisní činnosti povinen zajistit bezplatně kybernetickou bezpečnost na zadavatelem stanovenou minimální úroveň (např. prostřednictvím dodání a instalace dalších bezpečnostních prvků ve vztahu k možnosti setrvání připojení dodaného zařízení k síti zadavatele).

s) Veškerá vzdálená správa dodávaných systémů musí být řízená VPN a firewallem zadavatele. Jakékoliv vzdálené řízení výpočetní techniky programy typu TeamViewer, LogmeIN nebo podobné je nepřípustné.

t) Instalace serverů a IT techniky do serveroven v prostředí FN HK se řídí jiným standardem. K dispozici je na vyžádání prostřednictvím e-mailu helpdesk@fnhk.cz na základě prohlášení o mlčenlivosti

V případě, že dodavatel nemůže tyto standardy dodržet (z technologických důvodů), musí být realizována takové opatření, aby byly naplněny požadavky kybernetické bezpečnosti. Na odchylky proti standardu je třeba v nabídce zařízení zřetelně upozornit. Toto upozornění nezakládá automatické udělení výjimky a akceptaci nabídky.
Zejména:
Pokud nelze počítač/zařízení spravovat centrálním desktop managementem, musí dodavatel zajistit minimálně 2x ročně aktualizaci dostupných aktualizací výrobce operačního systému a aplikace na vlastní náklady.
Pokud řídící počítač systému nelze připojit do MS AD a dodavatel zajistí, na své náklady, řešení tohoto bezpečnostního problému (např. další PC součástí MS AD zajišťující předávání dat) tak, aby byl v souladu s kybernetickým zákonem. Toto řešení bude podléhat stejným SLA jako dodaný systém.
Pokud počítačový systém/dodaný SW vykazuje známé bezpečnostní chyby, které nelze opravit bezpečnostními záplatami nebo aktualizacemi, dodavatel doplní lokální firewall s logováním přístupu a napojením na centrální SIEM FN HK na vlastní náklady.
Pokud nelze na počítači/zařízení pracovat s doménovými účty s právy USERS bude ve spolupráci s OVS zakázán přístup počítače na internet. Pokud technologie potřebuje přístup na Internet, dodavatel musí specifikovat cíl přístupu pomocí FQDN (např. www.nejlepsilaborator.cz).
Lokální účet s právy USERS nutný pro běh systému musí odpovídat bezpečnostním standardům FNHK, délka minimálně 12 míst, velká a malá písmena, čísla, spec. znaky, změna hesla minimálně 1x za 18 měsíců zajistí dodavatel ve spolupráci s oddělením, na kterém je zařízení instalováno.
Pokud nelze na počítači/zařízení provozovat antivirový program FN HK, dodavatel zajistí softwarové vypnutí volných USB portů.
Pokud výrobce nepovoluje integraci se systémem SIEM (pro windows IBM WINCOLLECT, pro linux doplnění cíle syslog serveru) bude technologie izolována v datové síti firewallem zadavatele.
Pokud výrobce nepovoluje ICMP PING, musí uchazeč akceptovat bezplatné výjezdy techniků při problémech na datové síti.
Zkratka SIEM znamená: Security Information and Event Management jedná se o management bezpečnostních informací a událostí viz https://cs.wikipedia.org/wiki/Security_Information_and_Event_Management

Zkratka ICMP znamená: *Internet Control Message Protocol* - se používá v síti pro odesílání služebních informací, například chybových zpráv pro oznámení, že požadovaná služba není dostupná nebo že potřebný počítač není dosažitelný. ICMP – Wikipedie (wikipedia.org)