

Příručka kvality ICT

Datum vydání: 23. 4. 2025

Verze: 02

Počet stran: 20

Autor: **Mgr. Tomáš Kovařík**
Manažer kybernetické bezpečnosti

Garant: **Mgr. David Zažímal**
Náměstek informatiky a kybernetické bezpečnosti

Schválil: **Ing. Alexander Filip**
Ředitel
Nemocnice Jihlava, p. o.

Obsah

1.	ÚČEL.....	4
2.	PLATNOST	4
3.	POUŽITÉ ZKRATKY A POJMY	4
4.	EXTERNÍ BEZPEČNOSTNÍ POLITIKA	5
5.	ODBORNÍ GARANTI	5
6.	DOSTUPNÉ INFRASTRUKTURNÍ PRVKY NEMJI	5
6.1.	DATOVÉ CENTRUM	5
6.2.	V SAN	5
6.3.	DATABÁZE	5
6.4.	AZURE	5
7.	OBEČNÉ POŽADAVKY	5
8.	VZDÁLENÝ PŘÍSTUP	6
9.	OBLAST PACS	6
9.1.	DOKUMENTACE K ZAŘÍZENÍ	6
9.2.	OBEČNÉ POŽADAVKY NA DODÁVANÉ ZAŘÍZENÍ	7
9.3.	PŘÍSTUPOVÁ PRÁVA	7
9.4.	PŘIPRAVENOST PŘIPOJENÍ	7
9.5.	ZÁKLADNÍ POŽADAVKY NA DICOM ZAŘÍZENÍ	7
9.6.	DALŠÍ POŽADAVKY NA DICOM ZAŘÍZENÍ	7
10.	PŘIPOJENÍ ZDRAVOTNICKÉHO PŘÍSTROJE	8
10.1.	SPRÁVA PŘÍSTROJE A VZDÁLENÝ PŘÍSTUP K PŘÍSTROJI DODAVATELEM	8
11.	LICENCE NA UŽÍVÁNÍ SOFTWARE	8
11.1.	POVINNOSTI A ZÁVAZKY DODAVATELE LICENCÍ NA UŽÍVÁNÍ SOFTWARE	8
11.2.	POŽADAVKY NA LICENCE NA UŽÍVÁNÍ SOFTWARE	9
11.3.	POŽADAVKY NA PŘEDÁNÍ LICENCÍ NA UŽÍVÁNÍ SOFTWARE	10
11.4.	POŽADAVKY NA NABÝVACÍ DOKLADY K LICENCÍM NA UŽÍVÁNÍ SOFTWARE	10
12.	LOKÁLNÍ POČÍTAČOVÁ SÍŤ	10
12.1.	STRUKTUROVANÁ KABELÁŽ	10
12.2.	OPTICKÁ KABELÁŽ	11
12.3.	DATOVÉ ROZVODNY	12
13.	KONCOVÁ ZAŘÍZENÍ	12
13.1.	MINIMÁLNÍ POŽADAVKY NA PC	12
13.2.	POŽADAVKY NA TISKÁRNY	13
	<i>Fyzické a síťové připojení</i>	13
	<i>Podpora SNMP</i>	13
	<i>Konfigurace a instalace ovladačů v Microsoft Windows</i>	13
	<i>Bezpečnostní požadavky</i>	13
	<i>Diagnostika a správa</i>	13
13.3.	ZÁLOŽNÍ ZDROJE (UPS)	13
13.4.	ATS 16 AMP S KOMUNIKACÍ LAN SNMP:	13
13.5.	MANAGED AKTIVNÍ PRVKY	13
13.6.	BEZDRÁTOVÁ SÍŤ	13
13.7.	KAMEROVÝ SYSTÉM	14

13.8.	PŘÍSTUPOVÝ SYSTÉM.....	14
13.9.	PARKOVACÍ SYSTÉM.....	14
14.	PRACOVNÍ POSTUP	14
14.1.	SCHVALOVÁNÍ DOKUMENTACE	16
15.	CENTRÁLNÍ SIEM LOGMANAGER	16
16.	PRTG	16
17.	DATAWAREHOUSE	16
18.	OBLAST FONS	17
19.	SOUVISEJÍCÍ DOKUMENTY	17
20.	PŘÍLOHY.....	17
20.1.	REPORT O STAVU SYSTÉMU	17
20.2.	POSOUZENÍ SOULADU S PŘÍRUČKOU KVALITY ICT	19
20.3.	IMPLEMENTAČNÍ LIST PACS.....	20

1. Účel

Účelem tohoto dokumentu je definovat standardy dodávek a provozu na úseku ICT v NemJi. [Nemocnice Jihlava, o. o., podléhá zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, jakožto provozovatel základní služby poskytování zdravotní péče. V souladu s tímto zákonem má nemocnice implementovaný certifikovaný systém řízení informační bezpečnosti \(ISMS\) dle normy ISO 27001:2013. Tento systém garantuje vysokou úroveň ochrany citlivých dat, efektivní řízení rizik a plnění všech zákonných požadavků.](#)

2. Platnost

Tento dokument je platný a závazný pro všechny dodavatele a to ve verzi platné v době uzavření smlouvy a do doby vydání nové verze [tohoto](#) dokumentu. Všechny verze jsou umístěny na webových stránkách NemJi na adrese www.nemji.cz/pkict.

Nová verze vždy ruší platnost předcházející verze ke dni schválení a vystavení.

Vyjimky z této příručky kvality ICT jsou přípustné pouze po předchozím projednání a písemném odsouhlasení obou stran.

3. Použité zkratky a pojmy

AD – Active Directory (správa domén NEMJI)
AV – Anti Virus (antivirové zabezpečení)
CA – CyberArk (přístup k aktivům prostřednictvím PIM/PAM systému)
DCS – Dicom Conformance Statement (prohlášení o shodě s Dicom standardem)
Dicom – Digital Imaging and COmmunication in Medicine (standard pro přenos obrazové dokumentace)
HD – Helpdesk NEMJI
HIS/NIS – Hospital Information System / Nemocniční Informační Systém
HL7 – Health Level 7 (komunikační protokol pro přenos textové dokumentace HIS/NIS systémy)
ICT – Úsek informačních systémů
IS – Informační systém obecně
LAN – Local Area Network (místní síť NEMJI)
LIS – Laboratorní IS
MAC – Media Access Control address (unikátní identifikátor síťového rozhraní)
Mbps – Megabit per second (rychlost přenosu po síti)
MKB – manager kybernetické bezpečnosti
Modalita – zařízení používané v Radiologii pro snímkování pacientů
NemJi – Nemocnice Jihlava, příspěvková organizace
OSHW – Oddělení Správy Sítí a Hardwaru
PACS – Picture Archiving and Communication System (archivační systém obrazové dokumentace)
PC – Osobní počítač
PKICT – Příručka kvality ICT
Vendor – Dodavatel a/nebo suportní firma pro dodávané zařízení
VPN – Virtual Private Network (přístup do sítě NEMJI z internetu)
WAN – Wide Area Network
ZP – Zdravotnický přístroj

4. Externí bezpečnostní politika

Aktuální verze bezpečnostní politiky je dostupná na webových stránkách nemocnice:

<https://www.nemji.cz/kvalita/bezpecnost/>

5. Odborní garanti

Kontaktní informace lze nalézt na webových stránkách nemocnice: <https://www.nemji.cz/kontakty/usek-ict/> a <https://www.nemji.cz/kontakty/technicky-usek/>

6. Dostupné infrastrukturní prvky NEMJI

6.1. Datové centrum

Moderní datové centrum, 11 racků se studenou uzavřenou uličkou. Přívod el. 3fázový, rozdělený v racích na 2 větve, jedna větev za UPS. Celkově zálohováno centrálním dieselagregátem.

UPS 3x30kVA, chlazení duální 2x typ VERTIV PX051, EZS ústředna SATEL, SHZ ústředna KlikaBP SHZ EX 3001 se třemi konvenčními detekčními zónami, jednou záplavovou a zásobníky plynového hasiva FM200. Přístup do DC a racků je chráněn identitní bezkontaktní čipovou kartou a kamerovým systémem.

6.2. vSAN

V DC je VMware vSAN (software-defined, enterprise storage) nasazen prostřednictvím 6ti serverů na AMD EPYC 32C procesorech, per node 1024GB RAM a 64TB NVMe Enterprise datastore. Konektivita v rámci vSAN 100Gb/s.

6.3. Databáze

Microsoft SQL Server Enterprise: Core-based licensing s Always On High Availability (Availability Groups). – jen v případě lokalizace SQL na stávajících SQL clusterech NEMJI.

V případě dodávky zařízení či systému, který využívá databáze Microsoft SQL Server, NEMJI preferuje umístění databáze na již provozovaném Microsoft SQL Clusteru s vysokou dostupností (v již existující instanci Microsoft SQL Server verze 2019 nebo vyšší, s ověřováním uživatelů vůči databázi výhradně s využitím účtů a skupin v AD). Neposkytujeme roli „sysadmin“, standardně poskytujeme roli „dbcreator“.

Pokud bude dodávaný systém vyžadovat existenci vyhrazeného databázového serveru, musí být součástí dodávky potřebné licence Microsoft SQL Server, a to včetně potřebného počtu MS SQL Server CAL.

6.4. Azure

Disponujeme vlastním prostředím v Azure public cloudu a nabízíme možnost nasazení aplikací a služeb v tomto prostředí. Podporujeme širokou škálu služeb dostupnou v rámci Azure Marketplace, které lze snadno nasadit a přizpůsobit konkrétním potřebám daného systému. Z kreditu nelze platit licenční software třetích stran, což může ovlivnit rozpočet na nasazení určitých aplikací. Abychom zajistili optimální využití prostředků a předešli neplánovaným nákladům, je nutné před implementací provést podrobnou analýzu provozních nákladů, která zahrne všechny aspekty použití Azure prostředí.

7. Obecné požadavky

1. Pokud je součástí dodávky aplikační software, požadujeme, aby autentizace do aplikace byla řízena pomocí Microsoft Active Directory/Entra ID. Aplikace nesmí lokálně ukládat žádná hesla a autentizace musí proběhnout prostřednictvím protokolu Kerberos/SAML.
2. Pokud je součástí aplikační software, který umožňuje diferenciovat oprávnění v aplikaci, požadujeme, aby nastavení oprávnění v aplikaci bylo uděleno na základě členství ve skupině Microsoft Active Directory/Entra ID.

3. S ohledem na skutečnost, že Nemocnice Jihlava, příspěvková organizace je povinnou osobou dle Zákona č. 181/2014 Sb. požadujeme, aby veškeré logy ze všech aplikací a systému byly ukládány do centrálního logovacího a vyhodnocovacího systému SIEM.
4. Požadujeme plnou funkcionalitu všech dodávaných řešení minimálně na protokolech IPv4.
5. Požadujeme, aby součástí každého dodaného řešení byla možnost získat garantovanou dobu podpory s definovaným SLA minimálně po dobu následujících 5 let od dodávky takového řešení.
6. V rámci každé dodávky nového SW či HW bude posouzeno ze strany nemocnice, zda je požadavek na datový výstup do DWH NemJi.
7. Verze OS - v rámci instalace a dodávky nových HW a SW řešení je podporován pouze OS ve verzi, který má aktuálně podporu od výrobce daného OS a to s výhledem minimálně dvou let dopředu.
8. NemJi používá pro ochranu OS na koncových stanicích i na serverové infrastruktuře systém Microsoft Defender ATP. Instalace je vyžadována na všech podporovaných typech OS. Zajištění procesu nákupu a realizace (instalace) samotné licence je v režii ICT.
9. Pravidelné updaty a restarty (definovat servisní okno) – dodavatel je povinen na vyžádání provést potřebné updaty a opravy OS a dalších SW komponent, v případě, že bylo nalezena zranitelnost. V případě nahlášené zranitelnosti ze strany NemJi je dodavatel povinen provést nápravná opatření ke snížení rizik spojených s danou zranitelností, a to v co nejkratším možném termínu. Tyto služby musí být součástí servisní smlouvy.
10. Report o stavu systému – min. 4x za rok na adresu it-servis@nemji.cz. Tato služba musí být součástí servisní smlouvy. Jako vzor reportu je možné využít přílohu Report o stavu systému.
11. Součástí nabídky musí být predikce datového nárustu v horizontu 5 let – v případě nového systému.

8. Vzdálený přístup

Vzdálený přístup je zpravidla zprostředkován pomocí technologie PIM/PAM CyberArk Privilege Cloud.

Na základě schválené žádosti je uživateli odeslán uvítací e-mail s návodem na prvotní nastavení a použití vzdáleného přístupu. Přihlašovací jméno je součástí uvítacího e-mailu. Jednorázové heslo pro dokončení nastavení ze strany dodavatele je odesláno na telefonní číslo uvedené v žádosti.

Každý přístup dodavatele je monitorován PIM/PAM systémem. Ze strany Nemocnice Jihlava může dojít k aktivnímu monitoringu prováděné činnosti, případně k auditu již proběhlých činností.

Ve výjimečných případech, když není možné použít technologii CyberArk, je přidělován VPN přístup.

O zřízení vzdáleného přístupu dodavatele žádá vždy osoba z ICT, která je za daný systém odpovědná.

9. OBLAST PACS

V případě, že se jedná o Dicom zařízení, musí splňovat tzv. DCS (Dicom Conformance Statement). V případě, že toto zařízení nebude splňovat požadavky [této](#) PK, nebude implementované do infrastruktury NemJi.

9.1. Dokumentace k zařízení

Do termínu specifikovaného v harmonogramu implementace musí dodavatel vypracovat a předat příslušnému zástupci NEMJI detailní technickou dokumentaci k implementovanému zařízení a vyplněný implementační list dodaný garantem PACS (implementační list je v přílohách tohoto dokumentu). Tato dokumentace musí obsahovat provozní specifikace a nastavenou konfiguraci tohoto zařízení a ve zvláštním protokolu budou předána přístupová práva do instalovaného systému včetně administrátorského přístupu do systému.

9.2. Obecné požadavky na dodávané zařízení

Dodávané zařízení jakéhokoliv rozsahu musí splňovat alespoň základní požadavky dle technologického trendu obdobných zařízení na evropském a světovém trhu. Například pokud se jedná o zařízení používané v rámci NIS systému (i externě napojované), musí podporovat komunikační protokol HL7. Pokud se jedná o zařízení používané ke snímkování a radiologii, musí podporovat protokol Dicom. Všechna zařízení by měla být obecně schopná komunikace s okolními zařízeními podle mezinárodních standardů a schopná externí archivace dat.

9.3. Přístupová práva

Do dodávaného zařízení bude mít po skončené implementaci a příslušném zaškolení přístup specifikovaný počet osob s definovanými přístupovými právy. Tyto skupiny a jejich oprávnění budou specifikované v předávací dokumentaci. Za ICT musí být stanoven minimálně jeden správce resp. garant (případně zastupující správce), který bude dodavatelem řádně proškolen. Ze strany dodavatele bude v dokumentaci specifikována osoba (resp. osoby), které budou mít za účelem suportu administrátorský přístup do systému buď lokální anebo vzdálený. V případě dohody o používání vzdálené administrace pomocí CyberArk bude mít osoba provádějící suport přístup pouze na specifikované zařízení a tento přístup musí být logován. V případě, že některé oblasti proprietárního softwaru vyžadují přístup pouze administrátora ze strany vendora, budou tyto oblasti (např. adresáře, hivy registrů apod) oběma stranami konzultovány a vyspecifikovány v protokolu o zaškolení PACS administrátora NEMJI k danému zařízení.

9.4. Připravenost připojení

Dodavatel si musí ve spolupráci s příslušnými garanty ICT (LAN, AD a PACS) s dostatečným předstihem zajistit:

- Fyzické připojení do plánované lokality (síťové zásuvky, propojení na páteřní síť, požadovanou rychlost portu).
- Přidělení IP adresy resp. adres, hostname a AET dle jmenné konvence NemJi (hostname musí být shodný s AE title).
- Připravení registrace do OU v AD. Zároveň budou konzultovány aspekty doménové politiky, možnosti dálkové a lokální správy, autentizace přístupů, routování, apod.

9.5. Základní požadavky na Dicom zařízení

Modalita (Dicom node) musí:

- být kompatibilní minimálně se standardem **DICOM 3.0**,
- podporovat Dicom modalitu **WORKLIST** (MWL) a bezproblémově spolupracovat s NIS konektory,
- podporovat funkci **STORAGE COMMITMENT** při odesílání do PACS.

9.6. Další požadavky na Dicom zařízení

- Hostname a názvy nodů budou splňovat jmennou konvenci používanou v NemJi, přičemž v případě Dicom nodu **AET = Hostname**.
- Aplikační software ani rezidenční služby v operačním systému zařízení NESMÍ pracovat s právy lokálního administrátora, pouze s účtem s právy nezbytně nutnými pro provoz aplikace.
- Pokud jsou na bázi Windows, musí být připojeny do domény NemJi (Dicom nody např. formou autonomní OU „Modality“ podléhající pouze doménové politice, jejíž obsah bude dodavateli znám).
- Pokud jsou na bázi Windows, musí mít nainstalovaného AV klienta, instalaci klienta provádí příslušný správce AV řešení v NemJi na základě žádosti správce dané modality.
- Pokud systém podporuje zasílání logů musí být napojen na centrální Logmanager.
- Synchronizace času OS musí být zajištěna použitím doménového NTP serveru NemJi (ntp.nemji.cz).

- Dicom node/modalita bude po nakonfigurování posílat ve své Dicom hlavičce korektně těchto 5 standardních položek:
 - **ID Modality** (0008,0060) dle DCS (např. *MR*, pro magnetickou rezonanci atd.).
 - **ID StationName** (0008,1010) bude odpovídat přidělenému AET – Na všech modalitách musí tato položka obsahovat vlastní AET.
 - **ID InstitutionName** (0008,0080) bude nastaveno na: Nemocnice Jihlava, p.o.
- Dicom konfigurační mód bude zpřístupněn administrátorovi PACS z ICT a dodávající firma provede jeho zaškolení v oblasti příslušného Dicom nastavení dané stanice nebo serveru.
- Nastavení odesílání snímků a sérií musí být na modalitě nastaveno tak, aby primární destinace byla vždy centrální PACS NemJi, a až pak jako druhá (sekundární) destinace může být nastavena některá lokální stanice (např. diagnostická stanice na RDG nebo další vyhodnocovací SW).

10. Připojení zdravotnického přístroje

Dodavatel musí poskytnout přesnou specifikaci požadovaného připojení. Jasně popíše, co bude přistupovat do datové sítě Nemocnice Jihlava. Jaká zařízení budou dodána. Definuje požadavky, které jsou konkrétně k připojení vyžadovány (není možné poskytnout jen technickou dokumentaci dodávaného zařízení).

Dodavatel poskytne blokové schéma zapojení dodaného zařízení, včetně popisu síťové komunikace a potřebných protokolů a komunikovaných objemů dat.

Dodavatel popíše i požadavky na stavební připravenost pro připojení přístroje (zařízení), včetně potřebných podpůrných technologií (datová síť, počty datových zásuvek pro připojení atd.).

10.1. Správa přístroje a vzdálený přístup k přístroji dodavatelem

Dodavatel má možnost zařízení připojené do domény NEMJI spravovat vzdáleně, po schválení MKB. Pro zřízení přístupu do CyberArk NemJi je nutná příprava dokumentů pro vzdálený přístup. Pro ovládání přístroje přes RS232 nebo pro nedoménové přístroje, jsou popsány veškeré náležitosti, jež musí být splněny, v dokumentu <https://www.nemji.cz/kyberbezpecnost>.

11. Licence na užívání software

11.1. Povinnosti a závazky dodavatele licencí na užívání software

Dodavatel je povinen zahrnout do předmětu plnění všechny licence na užívání software (oprávnění k výkonu práva užívat software), které musí NemJi vlastnit pro provozování dodávaného zařízení či systému nebo jejich dílčích částí tak, aby zařízení či systém nebo jejich dílčí části užívala v souladu s platnou legislativou a licenčními ujednáními držitelů autorských práv k software, s výjimkou licencí na užívání software, který je využitelnou součástí stávajícího systémového prostředí informační infrastruktury NemJi. Využitelnou součástí stávajícího systémového prostředí informační infrastruktury NemJi jsou následující licence na užívání software:

- Microsoft Windows Server User CAL (v aktuálně provozované verzi v NemJi);
- Microsoft Windows Server Device CAL (jen u stávajících koncových zařízení zadavatele, na nichž má být využíván předmět plnění);
- Microsoft Windows Server DC (v aktuálně provozované verzi v NemJi) – jen v případě využití jako operačního systému virtuálního serveru, provozovaného na stávající virtualizační infrastruktuře NemJi, založené na platformě VMware;
- Microsoft SQL Server Enterprise Core (v aktuálně provozované verzi v NemJi) – jen

v případě lokalizace SQL databáze na stávajících SQL v HA;

- operační systémy Microsoft Windows Professional (povýšený NemJi na Enterprise) koncových zařízení (jen u stávajících koncových zařízení zadavatele, na nichž má být využíván předmět plnění).

Dodavatel zodpovídá za dodání licencí na užívání software v takových počtech a pro takové druhy, verze, licenční edice, licenční typy, bitové a jazykové mutace software tak, aby při provozování dodaného zařízení či systému nebo jejich dílčích částí požadovaným způsobem a v požadovaném rozsahu nedocházelo k porušování jakýchkoliv práv výrobců software, držitelů autorských práv k software nebo třetích stran.

Dodavatel se musí v nabídce i ve smlouvě zavázat, že dodané licence na užívání software budou prosté právních vad a zavázat se odškodnit v plné výši odběratele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady dodaných licencí na užívání software. V případě, že by nárok třetí osoby vznikl v souvislosti s dodávkou licencí na užívání software, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu (či obdobnému) zákazu či omezení využívání dodaných licencí na užívání software, musí se dodavatel zavázat zajistit náhradní řešení a minimalizovat dopady takovéto situace na odběratele, a to bez dopadu na kupní cenu, přičemž současně nebudou dotčeny ani nároky odběratele na náhradu škody.

11.2. Požadavky na licence na užívání software

Dodané licence na užívání software musí být určeny pro prodej v České republice, pro komerční organizaci (poskytující zdravotnické služby), být místně neomezené (případně místně omezené s právem jejich využívání v České republice) a být časově neomezené (trvalé). Pokud již trvalé licence na užívání určitého typu software nebudou dostupné, musí být dodány licence na užívání software časově omezené na období v trvání minimálně 60 měsíců. Dodávané licence na užívání software musí být nové, dodávka druhotných (použitých) licencí na užívání software se nepřipouští.

V případě dodávky licencí na užívání software společnosti Microsoft musí být dodány licence na užívání software v rámci některého typu multilicenční smlouvy společnosti Microsoft (dodávka licencí na užívání software v licenčních modelech OEM, FPP či licencování software jako služby nejsou až na níže uvedené výjimky přípustné). Dodavatel je povinen při dodávce licencí postupovat v souladu s pravidly společnosti Microsoft.

Výjimkou z požadavku na dodání multilicenčních licencí na užívání software společnosti Microsoft, krytých službou Microsoft Software Assurance, jsou:

- licence na užívání operačních systémů Microsoft Windows, které mohou být dodány jako licenční typ OEM (tedy jako nedílná součást zařízení, s nímž jsou dodávány) nebo jako plné licence (FPP);
- licence na užívání software společnosti Microsoft, dodávané jako nedílná součást zařízení, které je certifikovaným zdravotnickým prostředkem.

V případě, kdy dodávka obsahuje také koncové stanice (počítače, notebooky, tenké klienty apod.) s operačním systémem Microsoft Windows, musí být dodány s licencí na užívání operačního systému Microsoft Windows nejvyšší aktuálně uvolněné verze, v edici Professional nebo Enterprise, v licenčním typu OEM nebo jako plná licence (FPP).

NemJi preferuje řešení, jehož součástí není software založený na technologii Oracle Java, pro jehož užívání komerční společností jsou nezbytné placené licence. V případě, že součástí dodávky zařízení či systému musí být licence na užívání software, který využívá takové typy technologií Oracle Java, pro které musí mít komerční organizace licence na užívání Oracle Java, musí být součástí dodávky zařízení či systému také všechny potřebné licence na užívání Oracle Java. V případě instalace Oracle Java na server, dodavatel potřebný počet licencí pro servery navrhne na základě počtů a konfigurací dodávaných serverů (nebo stávajících serverů NemJi, určených NemJi k provozování systému), dle aktuálně platných licenčních podmínek společnosti Oracle. V případě instalace Oracle Java na zařízení (zdravotnický přístroj, počítač, notebook apod.) bude dodavateli oznámen počet zaměstnanců, kteří

budou daná zařízení používat (a budou tedy potřebovat uživatelskou licenci). V případě nedostupnosti trvalých licencí Oracle Java budou požadovány serverové i uživatelské licence na období minimálně 60 měsíců. Dodavatel je povinen při dodávce licencí na užívání software postupovat v souladu s pravidly společnosti Oracle.

11.3. Požadavky na předání licencí na užívání software

Pro každý jednotlivý typ licencí na užívání software, které budou součástí dodávaného zařízení či systému nebo jejich dílčích částí, musí dodavatel dodat licenční ujednání platné k datu dodání licencí na užívání software a všechny licenční materiály, které jsou nedílnou součástí daných licencí na užívání software (např. licenční číslo, licenční klíč, licenční certifikát, licenční oprávnění, štítek prokazující pravost licence, instalační média, hardwarový klíč, dokumentaci vztahující se k licenci apod.). Pokud k některé licenci na užívání software licenční ujednání neexistuje (držitel autorských práv licenční ujednání nevytvořil), musí být tato skutečnost výslovně uvedena na faktuře, dodacím listu, předávacím protokolu nebo akceptačním protokolu (alespoň na jednom z uvedených dokumentů). Nesplnění těchto podmínek bude v procesu akceptace dodávky klasifikováno jako podstatná (fatální) vada plnění (vada bránící následnému používání předmětu plnění).

11.4. Požadavky na nabývací doklady k licencím na užívání software

Daňový doklad musí obsahovat všechny náležitosti nezbytné k prokázání legálního nabytí licencí na užívání software, které budou součástí dodávky zařízení či systému nebo jejich dílčích částí. Minimálně musí pro každou licenci na užívání software obsahovat přesnou a úplnou specifikaci licence na užívání software (ve tvaru shodném s tím, jak licence na užívání software rozlišuje výrobce software - např. product number, výrobce software, název software, verze software, typ licence, jazyková mutace, bitová verze, časové omezení nebo další upřesňující údaje, jimiž výrobce software svoje licence rozlišuje), počet dodaných licencí (či vyjádření, že jde o licenci bez omezení počtu instalací nebo přístupů) a s výjimkou licencí, které jsou nedílnou součástí dodávaného zařízení a nemají stanovenou cenu (např. OEM licence operačního systému Microsoft Windows) také jejich cenu. Nesplnění těchto podmínek bude důvodem k vrácení daňového dokladu (faktury) k přepracování, přičemž lhůta splatnosti nového daňového dokladu (faktury) začne běžet dnem prokazatelného převzetí nového daňového dokladu (faktury) odběratelem.

12. Lokální počítačová síť

12.1. Strukturovaná kabeláž

- 1) V rámci prostor NemJi jsou definovány následující optimální standardy pro strukturovanou kabeláž:
 - Optimálně musí být instalována datová dvoj-portová zásuvka. Všechna zařízení, jež vyžadují datovou konektivitu, optimálně mají mít v největší blízkosti umístěnou datovou dvouportovou zásuvku (např. WiFi, TV, řídicí jednotky přístupového systému, kamery, zdravotnická technika, dohled měřicí a regulační technika atp.).
 - V rámci patientského pokoje standard je nutnost zajistit minimálně 1x datovou dvouportovou zásuvku na lůžko.
 - V rámci patientského pokoje intenzivní medicíny je nutnost zajistit minimálně 2x datovou dvouportovou zásuvku na lůžko.
 - Na každé pracoviště (pracovní místo s PC) musí být vždy instalovány minimálně 2x datové dvouportové zásuvky.
 - V rámci společných prostor zdravotnického zařízení (např. chodba ambulance) je nutné umístění minimálně 1x dvouportové zásuvky pro Wi-Fi na vzdálenost max 15 m mezi jednotlivými body a 1x jednoportové zásuvky pro kamerový systém na vzdálenost 20 m. V případě plánované instalace multimediální techniky optimálně umístění potřebných zásuvek dle instalace.
 - V rámci kancelářských prostor je nutné umístění minimálně 2x dvouportové zásuvky na jedno pracovní místo s tím, že na jedno

- pracovní místo se požaduje prostor 10 m².
 - V rámci vstupu do prostor budov vhodně umístit potřebné množství portů pro instalaci předpokládané techniky (IPTV, wifi, přístupový systém, kamerový systém).
 - Koncové zásuvky/keystone musí odpovídat vyžadované kategorii metalické kabeláže
- 2) Datové rozvody budou provedeny stíněnými kabely, v bezhalogenovém provedení vyhovujícím snížené hořlavosti a reakci na oheň dle vyhlášky č.268/2011Sb a dle ČSN EN 50575 v provedení B2ca - s1a, d1, a1, certifikaci CPR dle EN 60754-2, EN 61034-2 a integrovanému testu EN 50399. Instalační kabel min. Cat6A s garancí PoE přenosů typ 1-4 (dle IEEE 802.3bt).
 - 3) Součástí předání STK bude 1Gbps měření standardu Cat6A a protokoly z měření každého jednoho CAT6a portu, včetně patchpanelů a zásuvek.
 - 4) Datové zásuvky v jednotném bílém provedení, s popisnou plochou na označení.
 - 5) U nových rozvodů je preferováno připojení koncových telefonních přístrojů přes datové zásuvky. Pokud není v datovém rozvaděči připojen telefonní rozvod, je třeba v rámci projektu zajistit telefonní připojení do dotčených rozvaděčů o dostatečné kapacitě zakončených v Patch/Panelu koncovkami RJ45.

12.2. Optická kabeláž

Veškeré optické kabeláže se provádějí s využitím single mode (SM) 9/125nm min.G652D optických kabelů, s koncovkami SC/APC v optických vanách. Instalace včetně svařování požadovaných pigtailů, max. útlum sváru 0,15dB, max. útlum pigtailu 0,2dB. Na kabeláž bude poskytnuta záruka v délce min. 15 let garantovaná výrobcem.

Minimální počet optických vláken je 48 vláken pro propojení mezi serverovny v rámci budovy.

Propoje mezi budovami jsou vždy řešeny uvnitř budov nebo v zemi. Každá budova je připojena dvěma nezávislými cestami (které optimálně nejsou v souběhu blíže než 2 metry vně i uvnitř budovy).

Pokud půjde o operační sály nebo speciální pracoviště, bude optická infrastruktura řešena individuálně, podle požadavků techniky v daném místě vyžívané.

Ukončení optické kabeláže v optických vanách s koncovkami SC/APC, případně E2000/APC.

Optické kabely budou splňovat suchou, plně dielektrickou Loose Tube konstrukci standardního kabelu s LSOH UV stabilizovaným pláštěm, ochranou proti vlhkosti a vyhovující požární odolnosti IEC 60332-1 / IEC 60332-3 C / IEC 61034 a ochraně proti hlodavcům (např. vloženou vrstvou skelných elementů mezi jádrem a pláštěm kabelu). Vlákná budou chráněna tahovými členy a fixována v tahu např. aramidovými vlákny podél jádra kabelu.

Na každé trase SM (single-mode) vedení bude po realizaci provedeno standardní měření výkonovou metodou, zdroj světla 1310/1550nm s textovým vyznačením hodnot:

- Délka vlákna.
- Útlum celé trasy.
- Výpočet limitu útlumu trasy.

Budou provedeny případné zkoušky, revize, dodání příslušných dokladů, atestů, revizních zpráv, provozních řádů, prohlášení o shodě a dokladů o zkouškách (např. protipožární přepážky, atd.).

Každá trasa bude jednoznačně na čelním panelu optické vany označena dle požadavků oddělení OSSHW. Optické vedení bude označeno dle požadavků oddělení OSSHW.

Označení je možno provést na samotném kabelu, nebo kabelovými štítky po každých 5ti metrech vedení trasy.

Napojení a ukončení mikrotrubiček bude prováděno spojkami a ukončeními zabraňujícími průniku vody a hlodavců.

Při realizaci musí být dodrženy všechny požadavky výrobce optických kabelů (tah, ohyb atp.), legislativní a normativní povinnosti.

Minimální požární odolnost ucpávky EI30, součástí dodávky musí být prohlášení o shodě protipožárního systému, prohlášení o vlastnostech použitého materiálu a oprávnění výrobce protipožárního systému.

12.3. Datové rozvodny

Datové rozvodny musí být

- 1) Umístěny v každém patře zdravotnického zařízení Nemocnice Jihlava.
- 2) Napájeny ze dvou odpovídajících nezávislých elektrických zdrojů N+1. Napojení aktivních prvků na centrální UPS a ATS, nebo lokální UPS s dvojitou konverzí a lokální ATS. Monitoring (min. SNMP) stavu rozhraním Ethernet RJ45. Propojení UTP s datovým rozvaděčem (datová zásuvka).
- 3) Chlazeny min. z jednoho zdroje chlazení (zařízení pro trvalý provoz).
Klimatizace Specifikace
Parametry:
Chladicí výkon minimálně 2kW (zohlednit rozsah v daném projektu).
Chladivo R 32.
Nástěnné provedení.
Teplotní rozsah chlazení -15st až 47st vnější teploty. Funkce Auto restart po výpadku el. proudu.
Elektrický přívod ze sběrnice DO. Ovládání s ukazatelem teploty.
Provoz musí být zachován i při fungování jednoho zdroje chladu. Monitoring stavu a teplot rozhraním Ethernet RJ45.
- 4) Environmentální monitoring datové rozvodny – min. teplota místnosti, proudění a teplota vzduchu z chlazení, kouřové čidlo, výpadek napájení na nezálohované elektrické sítě.
- 5) Datový rozvaděč musí být umístěn tak, aby nebránil případné manipulaci při instalaci nových datových rozvodů. Datový rozvaděč bude o rozměrech minimálně 42U 19" 800x800 (pokud je to dispozičně možné), případně min. 600x600. Pokud je to prostorově možné, přední a zadní dveře perforované.
- 6) Elektrický přívod k racku: tři elektrické dvoj zásuvky jištěné C16A, ze sběrnice DO, elektro revize.
- 7) Do rozvaděče musí být přiveden odpovídající přívod elektrické energie, zásuvky typu E (CEE7/5).
- 8) Vstup do datové rozvodny přes ID kartu s PIN ověřením. V Nemocnici Jihlava je centrální přístupový systém od společnosti Cominfo, a.s. (www.cominfo.cz).
- 9) Prostor datové rozvodny požadujeme monitorovaný kamerovým systémem, dle kapitoly 10.5.
- 10) Naprosto vyloučeno je v daných místech mít vedeny rozvody vody, odpadů apod.
- 11) V případě, že by po instalaci pasivní části LAN nezbylo dostatečné místo pro instalaci adekvátní množství aktivních prvků, musí být pasivní část LAN rozdělena do více rackových skříní při zachování stejných parametrů.

13. Koncová zařízení

13.1. Minimální požadavky na PC

V okamžiku dodání požadujeme, aby dle CPUbenchmark.net splňoval procesor minimálně 20 000 bodů. Měl min 16 GB operační paměti a min. 500 GB SSD disk (M2.). Musí obsahovat licenci pro Windows 11 Profesional CZ.

13.2. Požadavky na tiskárny

Fyzické a síťové připojení

Specifikace Ethernet rozhraní (10/100/1000 Mbps).
Podporované síťové protokoly (TCP/IP, IPv4, IPv6).
Požadavky na kabeláž (kategorie kabelů CAT5e nebo vyšší).
Konfigurace IP adresy (statická nebo dynamická IP prostřednictvím DHCP).
Podporované porty a firewall pravidla (např. porty 9100, 161 pro SNMP, případně WSD).

Podpora SNMP

Verze SNMP, které tiskárna podporuje (min. SNMP v1, v2c).
Konfigurace SNMP komunity (např. možnost změnit výchozí komunitu „public“ a „private“).
Kompatibilitu monitorovacích a správcovských funkcí přes SNMP (např. stav tiskárny, úroveň toneru, chybové hlášení) s dohledovým systémem MyQ.

Konfigurace a instalace ovladačů v Microsoft Windows

Kompatibilní operační systémy (Windows 10 a vyšší).
Podrobnosti k instalaci ovladačů (PCL, PostScript, univerzální ovladače).
Postup pro konfiguraci tiskárny jako „Standard TCP/IP Port Printer“.
Nastavení ověřovacích parametrů (např. sdílení sítě, přístupová práva).

Bezpečnostní požadavky

Podpora konfigurace hesel pro správu přístupu k tiskárně a SNMP.
Podpora update firmware z WWW stránek výrobce.

Diagnostika a správa

Popis diagnostických funkcí a rozhraní pro monitoring tiskárny.
Návod na kontrolu a testování připojení a funkce tiskárny z Windows.
Návod na údržbu a update firmware.

13.3. Záložní zdroje (UPS)

UPS s dvojitou konverzí – Online.
Výkon minimálně 3000VA (zohlednit rozsah v daném projektu).
Rack provedení.
1 x PDU 16A/230V se zástrčkami CEE7/5.
SNMP v1, v2c výstup Ethernet RJ45LAN.

13.4. ATS 16 Amp s komunikací LAN SNMP:

Zatížení 16A.
Doba přepnutí Max 8 ms.
SNMP v1, v2c výstup Ethernet RJ45.
PDU 16A/230V se zástrčkami CEE7/5.

13.5. Managed aktivní prvky

Kompatibilní s danou síťovou vrstvou aktivních prvků CORE/AGREGACE/ACCESS, dle požadavku patřičného garanta za LAN/WAN/MAN/RAN odbornost Nemocnice Jihlava. Aktivní prvek musí být vybaven veškerým příslušenstvím pro zapojení k dané síťové vrstvě (optické kabely, napájecí kabely, laserové SFP/SFP+/QSFP/SFP28 moduly). Aktivní prvek, jenž bude dodán, musí být před nákupem konzultován s patřičným garantem za LAN/WAN/MAN/RAN odbornost Nemocnice Jihlava, včetně licenčních požadavků.

13.6. Bezdrátová síť

V rámci nových projektů je třeba počítat s instalací datových dvouzásuvek pro bezdrátové vysílače, které slouží pro bezdrátový přístup jak do LAN/WAN NEMJI. Datové dvouzásuvky je třeba umístit vždy

tak, aby byly co možná nejbližší k umístění bezdrátového vysílače. Datové dvouzásuvky pro bezdrátové vysílače je žádoucí instalovat nad podhled, pokud jsou k tomu podmínky. V současné chvíli je v Nemji používána technologie od společnosti Aruba HP. Pořizovat bezdrátové vysílače od jiných výrobců není možné, nejsou podporované centrálním kontrolerem. Nové bezdrátové vysílače tedy nepotřebují zásuvku na 220V. Vysílače jsou napájeny skrze POE aktivních prvků (switchů). Kompatibilní s danou síťovou vrstvou aktivních WiFi prvků a ověřovacích AAA aktuálně využívaných bezpečnostních mechanismů, dle požadavku patřičného garanta za WiFi odbornost Nemocnice Jihlava, včetně licenčních požadavků.

Vznik privátního APN neumožňujeme. Připojování probíhá prostřednictvím Policy enforceru implementovaného v rámci infrastruktury AAA ověřování uživatelů a zařízení na infrastruktuře Nemocnice Jihlava.

V případě realizace WiFi infrastruktury požadujeme měření na úrovni systému Ekahau, minimálně požadujeme reporty o rušení signálu, překážkách pro šíření bezdrátového signálu a úrovni šumu.

13.7. Kamerový systém

Centrálním kamerovým systémem NEMJI je software Milestone Expert (www.milestonesys.com).

Instalace nových či přemístění stávajících kamer musí odpovídat schvalovacímu procesu ICT.

U připojených kamer je zpravidla pořizován záznam (detekce pohybu), který je uchováván po dobu 30 dnů. Jsou podporovány pouze IP kamery Axis, které jsou kompatibilní s tímto kamerovým systémem, a které jsou zapojeny do jednotného managementu Axis device management. Pro přidání nové kamery do centrálního kamerového systému je třeba zakoupit k tomu potřebnou licenci do centrálního kamerového systému Milestone Expert (Milestone XProtect Expert Device License) včetně podpory (Milestone XProtect Expert Care Plus).

13.8. Přístupový systém

Centrální přístupový systém od společnosti Cominfo, a.s. (www.cominfo.cz). Jedná se bezkontaktní ID karty s RFID čipem. Řídící jednotky by měly být umísťovány do Datových rozvodů. Čtečky bezkontaktních karet musí být duální (pro frekvenci 125kHz a 13,56MHz). Dle specifikace dodavatele přístupového systému ([odkaz](#)) – Model „DUAL line“ nebo „Dual PIN line“. Do datových rozvodů musí být osazena Duální čtečka s číselníkem pro zadání PIN (Dual PIN line). Preferujeme černou barvu – pro udržení jednotnosti v organizaci.

Centrálním přístupovým systémem NEMJI je přístupový systém (SW ACCESS) od společnosti Cominfo, a.s., tedy není možná instalace jiných přístupových systémů. Základním komunikačním a řídicím prvkem systému ACCESS je řídicí jednotka, ke které jsou připojeny čtečky bezkontaktních karet. Je možné využívat pouze stávající ID karty.

13.9. Parkovací systém

Parkovací systém od společnosti Green Center s.r.o. (www.green.cz). Systém s automatickým rozpoznáváním RZ a dále možnost průjezdů na stejné ID s RFID čipem (ID karty). Čtečky musí být kompatibilní pro zapojení do parkovacího systému pro externí řízení přístupu – na frekvenci 13,56 MHz. Přesnější specifikace karty viz výše (Přístupový systém).

Centrálním parkovacím systémem Nemji je Parkovací systém Variant ([odkaz](#)) od společnosti Green Center s.r.o., tedy není možná instalace jiných parkovacích systémů.

14. PRACOVNÍ POSTUP

Projekční, realizační a montážní práce prováděné v rámci rozšíření stávajícího systému strukturované kabeláže (STK) a datovém rozvaděči (RACK) Nemji:

- 1) Před zahájením projekčních prací, je nutné předem kontaktovat oddělení OSSHW a konzultovat s ním veškeré požadavky vyplývající ze zadání objednatele, s dostatečným časovým předstihem, min. 7 prac. dnů.
- 2) Po zpracování a vyhotovení jakéhokoliv stupně projektové dokumentace vyplývající ze zadání objednatele, je nutné po zpracování předat tuto dokumentaci k vyjádření na úsek ICT Nemocnice Jihlava s dostatečným časovým předstihem, min. 7 prac. dnů.

- 3) Úsek ICT Nemocnice Jihlava se vyjádří ke zpracované projektové dokumentaci v zájmu společnosti a v rámci zachování jednotnosti a systémovosti daného systému STK, který je v prostorách zahrnující projektovou část již nainstalován. Projektová dokumentace bude obsahovat výkresovou a textovou část vč. úplných výkazů výměr a bude rozdělena na editovatelnou a needitovatelnou část. Projektová dokumentace bude předaná ve standardních formátech dwg, nebo dgn, příp. pdf, doc, xls. Případně další použitelné formáty budou konzultovány s oddělením OSSHW.
- 4) V rámci výběrových řízení, do nichž bude začleněn systém STK, budou do hodnotících komisí nominováni zástupci oddělení OSSHW, kteří budou mít povinnost v zájmu společnosti dbát na správnost hodnocení daného uchazeče, který se uchází o danou zakázku a který plně splňuje hodnotící kritéria dané zadáním a je plně oprávněn kvalifikačními předpoklady daný systém STK instalovat se zachováním systému záruky.
- 5) Vybraný uchazeč, který splnil veškerá kritéria výběrového řízení a který se v rámci kvalifikačních předpokladů zaručil, že dodrží veškeré body vyplývající ze zadání, je povinen v rámci realizačních prací plně spolupracovat s oddělením OSSHW od přípravných prací až po konečné předání projektové dokumentace skutečného stavu vč. měřících protokolů.
- 6) Před zahájením instalačních prací je prováděcí firma povinna předložit plán případných změn oproti předané projektové dokumentaci, katalogové listy od dodávaných komponentů a předložit formulář o kalibraci měřícího přístroje.
- 7) Při montážích prací v datovém rozvaděči, musí instalační firma dbát zvýšené ostražitosti a nesmí nikterak omezit provoz způsobený odpojením nebo poškozením stávajících zařízení vč. kabelových propojení.
- 8) Při montáži nových datových zásuvek musí instalační firma plně respektovat stávající použitelné komponenty a musí dodat takové, které budou barevně a kvalitou na stejné úrovni nebo vyšší.
- 9) Nová kabeláž, která bude instalovaná do stávajících kabelových tras, musí být před ukončením montáže vizuálně zkontrolována a její správnost odsouhlasena zástupcem zadavatele. Nová kabeláž zatahovaná do stávajících datových rozvaděčů musí být systémově přichycena a vyvážána.
- 10) Při montáži nových datových rozvodů do datového rozvaděče (rack) musí instalační firma plně respektovat stávající použitelné komponenty. V případě nově instalovaných patch panelů, či vkládání nových konektorů RJ45 do stávajících patch panelů, musí být zachován stávající standard, tzn. používat stejné patch panely vč. příslušných konektorů RJ45, jako jsou používány doposud.
- 11) V případě, že v rámci projektu bude dodán nový datový rozvaděč, musejí být splněny následující požadavky – viz kapitola 9.3 Datové rozvodny.
- 12) Oddělení OSSHW musí mít do datových rozvodů přístup 24/7.
- 13) Pokud je prováděna v technické místnosti s datovými rozvaděči jakákoli práce způsobující v ovzduší nečistoty, musí být zabezpečeno, aby nedocházelo k jejich šíření (musí být zajištěna bezprašnost prostředí).
- 14) Po dokončení prací, nesmí zůstat v místnosti nepořádek a datový rozvaděč i jeho okolí musí být zhotovitelem po úkonu řádně uklizené. V opačném případě nebude dílo převzato.
- 15) Pokud je prováděna jakákoli manipulace se stávajícími datovými rozvody (demontáž dat. zás., přesun dat. zás. atp.), tak je nutné tyto rozvody zachovat. Zachování stávajících rozvodů by mělo být provedeno, buď stočením kabeláže např. do podhledů, nebo jejich použitím k nově zřizovaným zásuvkám v případě, že splňují výše popsané standardy. V obou případech je nutné zachovat stávající popis, jak v datovém rozvaděči, tak na dat. zásuvce. Po takto provedené manipulaci musí být tato změna zanesena do výkresové části a tyto zásuvky musí být řádně proměřeny za účelem prokázání jejich funkčnosti. Pokud zachování stávající kabeláže nebude z jasně definovaných důvodů možné, je zhotovitel povinen tuto kabeláž demontovat v celé její trase, až do datového rozvaděče. Bližší konzultace by měla být prováděna s kontaktní osobou objednatele.
- 16) Při zhotovení nové datové zásuvky musí být tato zásuvka adekvátně označena na obou koncích stejným označením dle stávajících standardů (popisek datové zásuvky

nesmí být v rámci budovy duplicitní). Zásuvka musí být zakreslena do projektové dokumentace skutečného provedení. Každý vývod datové zásuvky je označen.

- 17) Všechny úkony spojené se změnou konfigurace sítě a správy sítě se budou provádět pouze v datových rozvaděčích, umístěných v předepsaných a schválených místnostech. Na panelu je každý vývod označen štítkem. Pro propojování na panelu budou použity propojovací kabely ukončené na obou koncích konektory RJ45. Uspořádání síťových komponentů v datových rozvaděčích jsou na výkresech čelních pohledů na datové rozvaděče, kterých je součástí projektové dokumentace skutečného provedení.
- 18) Po provedené montáži musí instalační firma provést měření datových vývodů, ze kterého musí sestavit a předložit certifikovaný měřicí protokol za každý jeden datový spoj či dvojici konektorů.
- 19) Veškeré dodané a instalované komponenty musí být nové a nepoužité.
- 20) Pokud je v rámci projektu řešena zcela nová datová rozvodna, je třeba počítat i s dalším rozšířením. Tedy rozměry místnosti dle místa (budovy) minimálně možnost instalace dvou racků, včetně manipulačních prostor kolem nich. Případně vždy možnost přidání jednoho dalšího racku.
- 21) Prováděcí firma je povinna provést po ukončení všech montážní činností závěrečný úklid, předat zpět veškeré zapůjčené materiály a předat projekt skutečného stavu v datové i papírové formě v předepsaných formátech vč. certifikovaného měřicího protokolu.

V případě porušení výše uvedených ustanovení, nebude zhotovená práce převzata a takto provedená práce bude brána jako hrubé porušení stanov pro práci v rámci Nemocnice Jihlava na rozšíření stávajícího systému strukturované kabeláže.

14.1. Schvalování dokumentace

Každý stupeň projektové dokumentace musí být schválen Úsekem ICT a předložen s dostatečným předstihem 7 prac.dnů.

15. Centrální SIEM Logmanager

Každý systém připojený do sítě NemJi musí zasílat logy do centrálního SIEM. Rozsah logů musí být v souladu se Zákonem č. 181/2014 Sb. o kybernetické bezpečnosti (dále jen ZKB) a Vyhláškou č. 82/2018 Sb. o kybernetické bezpečnosti (dále jen VKB).

SIEM Logmanager podporuje širokou škálu logů. Nastavení logování jednotlivých typů lze dohledat v oficiální dokumentaci systému: <https://doc.logmanager.cz/manual/lm/cs/devices/index.html>.

U zdravotnických modalit preferujeme logování dle Integrating the Healthcare Enterprise (IHE) Audit Trail and Node Authentication (ATNA) standardu, který podporuje bezpečnost a sledovatelnost dat v oblasti zdravotnické informatiky. Standard ATNA zajišťuje konzistentní přístup k auditování a autentizaci mezi systémy v rámci zdravotnických organizací, aby bylo možné sledovat přístup k citlivým informacím, jako jsou zdravotní záznamy pacientů.

16. PRTG

Každý systém připojený do sítě NemJi musí mít nastaven provozní monitoring v centrálním PRTG. Rozsah monitorovaných služeb je nezbytné v rámci implementace vždy sdělit, nutné je vždy konzultovat se správcem PRTG.

Oficiální dokumentace PRTG: https://www.paessler.com/manuals/prtg/welcome_to_prtg.

17. DataWarehouse

Pokud má dodávaný systém reportovat data do DW, je třeba aby splňoval požadavky na připojení do Microsoft Fabric viz. (Primárně - [Data pipeline connectors in Microsoft Fabric - Microsoft Fabric](#) |

[Microsoft Learn](#), sekundárně i možnost připojení přes [Dataflow Gen2 connectors in Microsoft Fabric - Microsoft Fabric | Microsoft Learn](#)).

18. Oblast FONS

Pokud má dodávaný systém (SW/HW) komunikovat či předávat data s NIS FE, je nezbytné, aby bylo součástí nabídky a dodávky vyřešené datové a komunikační rozhraní včetně všech potřebných licencí.

19. Související dokumenty

Ř 034 Bezpečnostní politika Nemocnice Jihlava – externí.

20. Přílohy

20.1. Report o stavu systému

1. Úvod.
 - Stručný popis obsahu reportu.
 - Doba, za kterou report platí (čtvrtletí).
 - Datum vytvoření reportu a kontaktní informace na zodpovědnou osobu.
2. Souhrn stavu systému
 - Celkový přehled stavu systému (např. provozuschopný, se zvýšeným rizikem, vyžadující zásah).
 - Shrnutí klíčových parametrů výkonnosti (dostupnost, výkon, bezpečnostní úroveň).
 - Zpráva o celkovém zdraví systému.
3. Přehled provedených změn.
 - Detailní popis všech změn provedených od předchozího reportu (aktualizace softwaru, konfigurace, záplaty).
 - Datum a důvod každé změny.
 - Informace o možném dopadu změn na provoz systému.
4. Detekované bezpečnostní hrozby (KBU/KBI).
 - Přehled kritických bezpečnostních událostí (KBU – kritická bezpečnostní událost).
 - Přehled významných bezpečnostních incidentů (KBI – bezpečnostní incident).
 - Popis, jak byly tyto události detekovány a vyřešeny.
 - Doporučení pro posílení zabezpečení na základě zjištěných událostí.
5. Doporučení na upgrade systému.
 - Doporučení na aktualizaci softwaru (včetně operačního systému a aplikací).
 - Doporučení na hardwarové upgrady pro optimalizaci výkonu nebo zajištění souladu s bezpečnostními normami.
 - Návrh na implementaci nových technologií nebo funkcionalit, které mohou zvýšit efektivitu nebo bezpečnost.
6. Doporučení na výměnu nebo údržbu hardware.
 - Stav hlavních hardwarových komponent (např. servery, úložiště, síťové prvky).
 - Doporučení na výměnu komponent, které dosahují konce své životnosti nebo vykazují známky opotřebení.
 - Doporučení na plán preventivní údržby.
7. Přehled plánovaných změn a údržby (následující období)
 - Seznam plánovaných změn a údržby pro následující čtvrtletí (aktualizace, bezpečnostní záplaty, upgrady).
 - Plán činností s časovým rozvrhem a předpokládanými dopady na provoz systému.
8. Další doporučení.

- Další doporučení na zlepšení systémového prostředí, zvýšení bezpečnosti nebo zlepšení výkonu.
 - Doporučení na školení či osvětu uživatelů, pokud by zlepšila celkový stav systému.
9. Závěr.
- Souhrn nejdůležitějších informací z reportu.
 - Krátkodobé a dlouhodobé návrhy na další kroky.
10. Přílohy.
- Technické detaily (např. podrobné logy, výsledky monitorovacích nástrojů).
 - Další dokumenty, které jsou relevantní k předchozím sekcím.

20.2. Posouzení souladu s Příručkou kvality ICT (vyplňuje dodavatel – příloha nabídky)

Požadavek	Splněno (Ano/Ne)	Podrobný (ideálně technický) popis splnění požadavku nebo odkaz na nabídku, kde je uvedeno
1. Přístupová oprávnění do aplikace řízena pomocí Microsoft Active Directory/Entra ID		
2. Nastavení oprávnění v aplikaci na základě členství ve skupině Microsoft AD/Entra ID		
3. <u>V rámci dodávky dojde k</u> ukládání logů do centrálního logovacího systému SIEM Logmanager		
4. Plná funkcionality na protokolech IPv4		
5. Garantovaná doba podpory <u>dodávaného řešení</u> s definovaným SLA <u>je</u> na min. 5 let		
6. <u>Možnost</u> datového výstupu do DWH NemJi při každé dodávce nového SW/HW		
7. <u>V rámci dodávky bude realizována</u> instalace pouze OS verze s aktuální podporou výrobce, min. s výhledem na 2 roky dopředu		
8. <u>Je umožněna</u> Instalace Microsoft Defender ATP na všech <u>dodávaných a</u> podporovaných OS		
9. <u>Součástí servisní smlouvy jsou ze strany dodavatele zajištěny pravidelné</u> updaty a restarty dle servisního okna na vyžádání		
10. <u>Součástí servisní smlouvy je zajištěn</u> „Report o stavu systému“ min. 4x ročně		
11. Predikce datového nárůstu v horizontu 5 let		
12. <u>Vyjádření</u> dodavatele <u>k</u> bodům, které jsou v <u>nesouladu s PKICT</u> včetně návrhu opatření		

20.3. Implementační list PACS

Implementační list připojení DICOM modality

Dodavatel:				Vyplní			
Typ přístroje:				MAC adresa			
Typ modality				Interní IP		ANO ☐ NE ☐	
Lokální storage		ANO ☐ NE ☐		Interní IP			
IP				NETMASK			
GW				DNS 1			
HOSTNAME:				DNS 2			

Požadované služby:	1	DICOM STORAGE		
		Typ modality		Dodavatel
		AE TITLE		Dodavatel
		Privátní SOP	ANO* ☐ NE ☐	Dodavatel
	2	DICOM STORAGE COMMITMENT		
		AE TITLE		Dodavatel
		Commitment port		Dodavatel
	3	DICOM MODALITY WORKLIST		
		AET		Dodavatel
		Zkratka v NIS		NEMJI
		Pracoviště v NIS		NEMJI - OZM
	4	DICOM Q/R		
		AE TITLE		Dodavatel
		Lokální storage port		Dodavatel

LOCAL PACS		
PACS DICOM STORAGE SCP	IP	172.19.192.18
	AET	FUSION
	PORT	104
PACS MODALITY WORKLIST SCP	IP	172.19.192.18
	Port	4488
	AE TITLE	JIVEX_WL
PACS QUERY/RETRIEVE SCP	IP	172.19.192.18
	AET	JIVEX_QR
	PORT	4498

Query: study root

* V příloze uveďte seznam privátních SOP které chcete ukládat do PACS

Za dodavatele:		Za NEMJI:	
		IT:	
Jméno:		Telefon:	
Příjmení:		NIS:	
Telefon:		Telefon:	
Email:		Požadující odd:	
Podpis:		Telefon:	

DICOM atributy:

(0008,0080)

NEMOCNICE JIHLAVA, P.O.